Fall 8-1-2016

An Integrated Framework for the Recovery of Evidence from Encrypted Hard Disk Drives

Christopher Copeland
Dakota State University

AN INTEGRATED FRAMEWORK FOR THE RECOVERY OF EVIDENCE FROM ENCRYPTED HARD DISK DRIVES

A dissertation submitted to Dakota State University in partial fulfillment of the requirements for the degree of

Doctor of Science

in

Information Systems

August, 2016

By
Christopher Copeland

Dissertation Committee:
Dr. Ashley Podhradsky
Dr. Jun Liu
Dr. Kyle Cronin
Dr. Viki Johnson

DISSERTATION APPROVAL FORM

This dissertation is approved as a credible and independent investigation by a candidate for the Doctor of Science in Information Systems degree and is acceptable for meeting the dissertation requirements for this degree. Acceptance of this dissertation does not imply that the conclusions reached by the candidate are necessarily the conclusions of the major department or university.

Student Name: Christopher Copeland

Dissertation Title: An Integrated Framework for the Recovery of Evidence from Encrypted Hard Disk Drives

Dissertation Chair/Co-Chair: _____ Date: 8-9-16

Committee member: _____ Date: 08/09/2016

Committee member: _____ Date: 08/09/2016

Committee member: _____ Date: 8/9/16

ACKNOWLEDGMENT

I want to thank the committee for all of their efforts throughout this endeavor. Their support, feedback, and encouragement have been paramount to this success. Specifically, a sincere thanks and acknowledgement to Dr. Podhradsky for her commitment to this study. She was instrumental in this process from concept to completion and went above and beyond in handling the process with me.

I would like to thank my colleagues at the Tarrant County District Attorney's Office, Vincent Giardino and Kyle Gibson. Their efforts and feedback were critical as practitioners and experts in the field and helped shape the foundation of this study. I would also like to thank the efforts of the Dallas FBI for guidance on process and current case law. Dr. Rhonda Dobbs for her continued friendship and support for 11 years. Thank you for giving me feedback, lifting my spirits, and reminding me that life exists outside a dissertation process. Dr. Alex del Carmen, thank you for being my mentor and friend these last 17 years. You encouraged me as an undergraduate student, guided me through a Master's program, and cheered me to finishing my graduate work. Thank you for all of your effort and for the believing in me. All the remaining faculty from Tarleton State University who supported and encouraged me along the way, thank you.

My Mother and Father, Francine and Michael, thank you for teaching me and allowing me to grow. You encouraged a life-long love of learning. You inspired me to keep going and to reach my dreams. Lastly, my wife Mariam. You have been the pillar and foundation of every achievement and goal these last 12 years. Without your support, kindness, and strength, none of this would have been possible. This document represents your sacrifice and dedication as much as it does mine. Thank you and I love you dearly.

ABSTRACT

The use of disk encryption has become more prevalent in recent years. As the ability to encrypt a logical and physical volume becomes easier for end users, the role of examiners becomes more difficult when conducting digital forensics investigations. The purpose of this research is to provide an integrative framework, which mitigates the risks of data access loss when performing a digital forensic investigation. The framework will include issues of legality as well as whole disk encryption integrating previous frameworks. The framework will then be validated against several scenarios in which encryption has been used.

DECLARATION

I hereby certify that this dissertation constitutes my own product, that where the language of others is set forth, quotation marks so indicate, and that appropriate credit is given where I have used the language, ideas, expressions or writings of another.

I declare that the dissertation describes original work that has not previously been presented for the award of any other degree of any institution.

Signed,

Christopher Copeland

TABLE OF CONTENTS

DISSERTATION APPROVAL FORM ..... **II**

ACKNOWLEDGMENT ..... **III**

ABSTRACT ..... **IV**

DECLARATION ..... **V**

TABLE OF CONTENTS ..... **VI**

LIST OF TABLES ..... **VII**

LIST OF FIGURES ..... **VIII**

INTRODUCTION **1**

BACKGROUND OF THE PROBLEM 1

STATEMENT OF THE PROBLEM 3

OBJECTIVES OF THE PROJECT 3

LITERATURE REVIEW **5**

RESEARCH METHODOLOGY **22**

RESULTS AND DISCUSSION **33**

CONCLUSIONS **41**

REFERENCES **47**

LIST OF TABLES

Table 1: EnFORZA Rubric 32
Table 2: Fricosu without EnFORZA 40
Table 3: Fricosu with EnFORZA 40

LIST OF FIGURES

Figure 1. Current Law Enforcement Best Practices 13
Figure 2. FORZA Process Overview by Ieong (2006) 19
Figure 3. FORZA High Level Overview by Ieong (2006) 20
Figure 4. Comparison of Best Practices and Proposed EnFORZA Framework 21

CHAPTER 1

INTRODUCTION

Background of the Problem

To the general Information Technology (IT) community, whole disk encryption has been viewed as a means to protect and secure data. From a law enforcement and digital forensics perspective, the challenges could be far more serious. Investigators that require the analysis of digital evidence must now take into consideration whole disk encryption methods and applications. What is more, there has been an explosion of disk encryption integration in recent years as both software and hardware implementations have been released for general consumer use in both traditional computing devices as well as the explosive mobile market. The consideration of encryption issues is seen in the relevant academic literature.

To have a meaningful discussion on whole disk encryption, the topic of encryption must first be examined. Unencrypted information is known as plaintext whereas encrypted information is known as cipher-text. Encryption is the process of making some form of information or data unreadable without a key. The process of encrypting information locks the information in an unreadable state. The only way to read or use that information is to decrypt it, or turn it into plain-text. The process of encryption relies on a mathematical algorithm. There are many various types and strengths of encryption algorithms available. Some of these algorithms are very strong in terms of keeping the encrypted or cipher-text from being decrypted through guessing or various cryptographic attacks.

The strength of the algorithm is typically relational to the length of the encryption key generated. Additionally, the encryption strength is also directly related to the number of times the plain text is run through the algorithm. As an example, the Advanced Encryption Standard (AES) algorithm uses a key length of 128 bits, would produce the cipher-text on round 10. The same algorithm with the same plain text would require 12 rounds on a 192bit key and 14 rounds on a 256bit key (*FIPS-197*, 2001). According to Schneier, the length of the key will depend entirely on the necessity and the value of the data encrypted. Different needs will

determine the algorithm and the key length selected to encrypted the plain-text (Schneier, 2007, pp. 166–167).

Although various algorithms can be used to protect data, a trend emerges when looking at the most common solutions for whole disk encryption. The AES standard is the most commonly used solution when it comes to imbedded encryption in an operating system as well as the most common commercial packages. Apple uses the AES-128 for the Apple Filevault 2 built into the OSX operating system (Apple Inc., 2012, p. 5). Microsoft Windows versions 7-10 uses AES with 128 or 256 bit keys ("BitLocker Drive Encryption in Windows 7: Frequently Asked Questions," 2012, "What's New in BitLocker," 2014; Lich, 2016). Red Hat Enterprise Linux supports the LUKS standard which operates with the AES algorithm at 256 or 512 bit keys (Fruhwirth, 2016; Krátký et al., 2016, p. 136). These represent the major operating systems used today in desktop and laptop computing. The inclusion of algorithms like AES has complicated matters for criminal investigators working with whole disk encryption.

One challenge with whole disk encryption (WDE) is that it is viewed as an anti-forensic tool. Meaning, it is an inhibitor to digital investigations and evidence collection. Another challenge is investigators do not always recognize when WDE has been used. The failure to recognize WDE is discussed in the literature review as well as the concerns with the use of dual encryption. Dual encryption techniques demonstrate the possibility of presenting fake or misleading data as a rising challenge to digital forensics investigators.

Traditionally, there has been a "pull the plug" approach when seizing and transporting a system. Removing the power to the system for seizure and transport would transition the system to the encrypted state, if WDE is used. The literature contains examples of determining the presence of cryptography and the presence of WDE, but so far, a fully formed framework for evidence collection has not been proposed with respect to the legality of encryption, issues of search and seizure, and data acquisition.

Of particular interest in the literature regarding WDE are the calls for research on this subject. Garfinkel describes the issues of WDE as a threatening denial of case data to investigators (Garfinkel, 2010). Casey and Stellatos discuss the rise in availability of WDE as an embedded option in modern operating systems (Casey & Stellatos, 2008). Several authors have put forth various artifacts in the literature which deal with the legality and acquisition of

data in digital forensic investigations (Altheide, Merloni, & Zanero, 2008; Carrier & Spafford, 2004; Ieong, 2006). What the literature lacks is design artifacts that incorporate more than key detection. Holistic and integrated approaches that include investigation, seizure, and legal issues with encryption considerations are lacking in the academic literature. Given the vacancy in the literature and calls for additional research, this paper will attempt to fill the void by presenting a design artifact for disk encryption.

Statement of the problem

With an increasing reliance on technology and the integration of that technology into the daily lives of consumers, there is a correlating increase in the recovery of technology in criminal investigations. In addition, there are established constitutional protections against illegal search and seizure as well as protections from self-incrimination. Changing privacy laws also complicate investigations as the court system adapts case law to changing technological environments. This leads to the primary research question. What considerations and resources are needed for the retrieval of evidence from encrypted hard disk drives in criminal investigations?

Objectives of the project

The primary purpose of this research is to provide a framework that takes into account the various considerations needed when conducting a digital forensics investigation in which WDE may be in use. These considerations include WDE, partial or protected volume encryption, and legal issues revolving around acquisition of data in digital investigations in the United States. Demonstration and evaluation of the artifact is a fundamental aspect to design science research. The purpose of the demonstration is to solve multiple instances of the identified problem (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007, p. 55). In relation to the issue of WDE, the artifact will be demonstrated against several common and industry standard scenarios. The evaluation process as described by Peffers et al. (Peffers et al., 2007, p. 56) will consist of artifact outcome comparison of the proposed artifact as well as other established frameworks discussed in the academic and best practices literature. Evaulation of the artifact will be based on the fifth evaluation technique proposed by Hevner et al. with

criminal event scenarios to demonstrate the artifact utility. If further iteration and refinement of the artifact is feasible, iteration will be performed.

CHAPTER 2

LITERATURE REVIEW

The literature regarding digital forensic investigations is sparse when dealing with WDE. The review of the literature is divided into areas of specificity with regard to WDE. These areas are a general discussion and calls for research in the area of WDE, deniable WDE, previous frameworks as digital forensic artifacts, previous methods and models as digital forensic artifacts, and current tools used in digital forensic investigations. The legal issues of discovery as well as search and seizure are discussed as part of the framework presented and will not be included in the review of the academic literature.

There has been a sharp increase in the number of civil and criminal cases in the United States in which digital and computer forensics are discussed (Losavio & Keeling, 2011, p. 2). This concern becomes complicated with the inclusion of encryption of hard disk drives used in these legal cases. Several of these cases have gone on to create legal precedence for recent investigations.

In 2006, Sebastien Boucher was investigated on charges of possession and transportation of child pornography into the United States from Canada. Immigration and Custom Enforcement (ICE) agents seized the laptop after viewing pornographic images on screen. Following the current law enforcement guidelines in the United States, the ICE agents powered down the laptop. When the laptop was powered on again, the drive containing the images in question was not accessible as it had been encrypted using full disk encryption. Boucher's attorney argued that providing the encryption passphrase would be a violation of his protection against self-incrimination as guaranteed by the United States Constitution. The United States District Court for the District of Vermont granted Boucher's motion to have the subpoena quashed in November 2007 (*In re Grand Jury Subpoena Sebastien Boucher*, 2007). On appeal, the subpoena was upheld reversing the quash motion and Boucher reached a plea arrangement with prosecution (*United States v. Boucher*, 2009).

The United States also sought prosecution against Thomas Kirschner for three felony counts of child pornography in 2009. Kirschner had already been indicted by a grand jury, and an additional subpoena was filed compelling Kirschner to provide any associated passwords to the computer in question. The files in question had been encrypted. Similar to Boucher, Kirschner also claimed Fifth Amendment protection against self-incrimination. The Federal Magistrate at the United States District Court of Michigan Southern Division agreed that the compelling of password would be akin to compelled testimony being given and would be a violation of the defendants Fifth Amendment rights (*United States v. Kirschner*, 2010).

In 2013, Ramona Camelia Fricosu had a Toshiba laptop seized by the FBI with a search warrant. When it was determined to be necessary, agents came back later with an additional warrant to search the contents of the encrypted laptop. When Fricosu's attorney withheld assistance, a motion was filed to compel a copy of the drive in an unencrypted format. The United States then used the All Writs Act of 1789 (*All Writs Act*, 1789) to require the defendant assist with the investigation. The judge in the case upheld this and the motion was granted (*United States v. Fricosu*, 2013). Prosecution later gained access to the password from a list provided by Fricosu's ex-husband, making the granted motion moot. Unlike previous cases, the avenue to compel here was not the same as in previous cases. Agents did not ask for a passphrase or encryption key, instead they focused on a compel order to deliver an unencrypted copy of the drive in question. By asking for the unencrypted copy as part of "assistance" to law enforcement, it allowed the defense counsel to choose the method of compliance and focuses on the outcome only. This circumvented the Fifth Amendment protections sought in Boucher and Kirschner. An interesting point in this particular investigation is that this is one of the primary avenues that the United States District Attorney's use to force decryption during an investigation by compelling assistance as compared to passphrases or decryption keys.

Leon Gelfgatt was indicted in 2014 on numerous charges of felony forgery and larceny. The state of Massachusetts filed a motion to compel Gelfgatt to supply his password for various electronic devices seized by investigators. The investigators seized several computers after following standard operating procedure for search and seizure. Forensic examiners were unable to view the files as they had been encrypted with DriveCrypt Plus ("Drive Crypt Plus," n.d.); the motion for compel was quashed by the judge in the case based

on Fifth Amendment protections. In appealing to the Massachusetts State Supreme Court, the prosecutors argued that the decryption would not release testimony information and reversed the quash motion (*Commonwealth v. Gelfgatt*, 2014). Unlike cases prosecuted at in the Federal District Criminal Court, this was a case in which prosecutors did not have access to more powerful legal tool like the All Writs Act of 1789 and had to rely on tools available to them at the state level. A concern becomes apparent when the current set of tools available to prosecution and investigators are not useful.

In some cases, investigators cannot compel the device owners to release the passphrase encryption key, or provide a copy of the unencrypted information. Ray Owens, a resident of the Chicago suburb of Evanston, was shot and killed in June 2015 (Seidenberg, 2015). Investigators found two smart phones with the body of Owens, an iPhone 6 and a Samsung Galaxy S6. Unfortunately, the phones were defaulted to the encrypted state. As state judge issued a warrant to order both Apple Inc. and Google Inc. to unlock the phones. Both companies responded that with the devices in the encrypted state, access to the information would be impossible (Vance, Molins, Leppard, & Zaragoza, 2015). A second case in Louisiana was very similar. On April 24, 2015, Brittney Mills a 29 year old of Baton Rouge was shot and killed along with her unborn son (Jones, 2015). Mills' smart phone was an Apple iPhone and was defaulted to the encrypted state making data retrieval impossible according to the authorities and Apple Inc. (Maddox, 2015). In cases where the owner of the device is deceased or missing, key and passphrase retrieval becomes significantly more difficult for forensic examiners, investigators, and prosecutors. This same issue would be no different had the devices been fully encrypted laptops or desktops.

This enhanced difficulty is the primary point of contention in an ongoing national legal battle in the United States. On February 16, 2016 the Federal Bureau of Investigation filed a motion in the United States District Court for the Central District of California to compel the computer and electronic company Apple Inc. to assist federal agents in an ongoing investigation related to the mass shooting by two San Bernardino terrorists in November 2015. At the core of the government argument is that Apple Inc. has created a device in which law enforcement cannot reasonably obtain evidence due to nature of device encryption and the protections built by Apple to unlock that encryption. Again, the United States Attorney is basing the request for assistance on the All Writs Act of 1789, but the concern is that the

assistance is very specific in nature. The FBI is asking for a revised version of the Apple iPhone Operating System, or iOS, without several of the security features that are publically available. The FBI lays out a methodical and established argument for Apple's compliance (*Government's Ex Parte Application for the Order Compelling Apple Inc. to Assist Agents in Search; Memorandum of Points and Authorities*, 2016).

Apple responded both publically and on appeal by stating a larger concern of government intrusion into privacy and backdoors into secure devices. In the appeal, Apple and other companies that support Apple, are concerned about the legal precedence being set that would allow technology companies and manufactures to be compelled by the United States to break or bypass the encryption of their own secure products. One of the legal arguments made by Apple goes back to *United States v. Fricosu*, in that it is legal for the Government to compel a defendant in a case, but compelling a third party in a criminal case has never been established in case law (*Apple Inc's Motion To Vacate Order Compelling Apple Inc. To Assist Agents In Search, And Opposition To Government's Motion To Compel Assistance*, 2016). The Government has focused on the arguments that this would only apply to one phone; that the All Writs Act does not preclude or disallow the compelling of a third party to assist; and that it would not create an undue burden on Apple to produce the modified iOS to law enforcement (*Government's Reply In Support Of Motion To Compel And Opposition To Apple Inc.'S Motion To Vacate Order*, 2016).While encryption is useful in protecting sensitive data such as health and financial information, the same technology can be utilized to thwart and prolong criminal prosecution as well as civil litigation. There is increased availability of commercial products as well as embedded FDE options in modern operating systems (Casey & Stellatos, 2008). Investigations in future instances will need to adapt to changing environments as disk encryption becomes more available. Casey et al. argue for increased and updated research to improve chances of evidence recovery in cases where WDE is utilized (Casey, Fellows, Geiger, & Stellatos, 2011). Garfinkel describes the rise in encryption as pervasive and complicating the process of forensic evidence (Garfinkel, 2010, p. 66). Joshi and Bhilare call for increased artifacts for digital forensic researchers and practitioners (Joshi & Bhilare, n.d., p. 296). In addition to the need for improved artifacts, there are also calls for research to assist with deniable encryption as an anti-forensic method

(Canetti, Dwork, Naor, & Ostrovsky, 1997; Garfinkel, 2010; Gasti, Ateniese, & Blanton, 2010; Grover, 2004, 2005).

The beginnings of consistent approaches to the extraction of digital evidence can begin with Mocas. Mocas outlines the underlying ideologies and abstractions for evaluation based digital forensics research (Mocas, 2004, p. 61). Beebe and Clark expanded on this foundation. They understood that the investigation process was complex and dynamic. Given this dynamic nature, various stages would be needed to complete the fundamental architecture of any forensic abstraction. Multi-tiered phases and sub-phases of the investigative process were proposed by Beebe and Clark with the goal of synergy with related artifacts and frameworks present in the scholastic literature (Beebe & Clark, 2005). This allowed each major phase to be further expanded and developed by other researchers. This expansion and development can be demonstrated by Ieong and the Forensic Zachman (FORZA) framework. Ieong argues that the forensic process will probably include various roles in its life-cycle. The FORZA framework includes these roles both inside and outside traditional computing related disciplines. Ieong accomplishes this with the inclusion of a legal viewpoint for the investigator (Ieong, 2006). Although the FORZA framework does include civil and criminal determination, it does not include recent legal considerations for encryption during seizure or discovery. Trček, Abie, Skomedal, and Starc proposed a top down framework for digital forensics that begins with legal issues and considerations with the intent to ease the selection of appropriate method for investigation (Trček, Abie, Skomedal, & Starc, 2010). This approach, which begins with legal concerns, is interesting given the changing landscape of privacy and technology in the United States.

The changing landscape of forensic investigations also includes discussion of live forensics. The majority of discussion regarding live forensics and disk encryption in the academic literature is centered on the notion of key determination and evidence acquisition. A primary contribution to this discussion in the literature is the Forensic Analysis Toolkit (FATKit) framework. The FATKit framework focuses on volatile memory and attempts to provide structure in the data gathered (Petroni Jr., Walters, Fraser, & Arbaugh, 2006). In addition to the contribution of Petroni et al. and their work on live forensics, the need to observe a live state is also important in digital investigations. Observing system memory content is crucial to determining encryption keys, passphrases, and currently running

processes. Chan presents a framework as Forenscope that allows investigators this level of observation of the machine live state but without altering memory content and jeopardizing the investigation (Chan, 2011).

The underlying basis for live forensics and practitioner tools is the foundation set forth by artifact design in the academic literature. The literature contains numerous models and discussions for research in digital forensic artifact design. In 2001, the Digital Forensic Research Workshop (DFRW) put forth a consensus document outlining what was needed for the field of study in digital forensics (Palmer, 2001). Although other models existed before the DFRW framework, this document is considered seminal as it was established by the attendees and practitioners in the field (M. M. Pollitt, 2007, p. 4). The DFRW framework was reviewed by Reith et al. in their discussion of various models as well. Reith et al. also discuss the issues in the field of digital forensics at the time of publication. One of these issues was the lack of standardization and consistency in the tools used in the forensic process; something echoed by the DFRW consensus document prior (Reith, Carr, & Gunsch, 2002). Although the frameworks presented at DFRW conferences have been updated and modified as various techniques and technology have become available, there has been little to no inclusion of full or whole disk encryption in the various submissions.

One of the issues of consistency plaguing digital investigations was the paradigm of the investigation process. Transitioning from a more traditional forensic process to a digital investigation process has beckoned the need for a paradigm shift on the parts of law enforcement, proprietary security, and contract security. There has been a need to bridge the distance between the traditional forensic process and the emerging dynamic of digital forensics. Models and frameworks that span this divide are provided in the literature with several major contributions by Carrier and Spafford.

Carrier and Spafford demonstrate an integrated model designed to bridge this separation between the two forensic processes. They accomplish this goal by altering the paradigm of the crime scene from a traditional viewpoint to a digital one through the utilization of the computer as the crime scene. The bridging artifact was designed to support both security and law enforcement based investigations (Carrier & Spafford, 2003). In addition, Carrier and Spafford later show that the event which triggers an investigation

typically requires an evidence basis in order to pursue future legal criminal or civil actions (Carrier & Spafford, 2004).

In addition, Carrier and Spafford later show the needs of investigators relating to event determination. The determination of an event that triggers a digital investigation requires an evidentiary basis needed for future legal action. Carrier argues that various abstraction layers should be used as a design artifact in the process of tool deconstruction. As tools are used in the forensic process, the understanding of abstraction layers within these tools will lead to better tool creation and development, and as an added result, better artifact creation (Carrier, 2003).

Baryamureeba et al. expanded upon the model put forth by Carrier and Spafford. They proposed the Enhanced Digital Investigation Process, an expanded model from the IDIP (Baryamureeba & Tushabe, 2004). The EDIP model includes more advanced and in-depth phases at each stage of the investigation. These advanced phases are a mechanism for the identification and collection of evidence of the primary and secondary crime scenes (Baryamureeba & Tushabe, 2004). The emphasis on the phases of an investigation process begins to show a need for further refinement of forensic based artifacts.

The literature includes several additional refinements of previous artifacts. One such refinement was put forth by Pollit. Pollit described a modified Zachman framework developed at the DFRW. This modified and refined framework shows a lack of consistency on the order in which the phases of a digital investigation work in a time sensitive manner (M. Pollitt, 2004). An interesting consideration to this model is the evolution of processes. Pollit argues that the evolution of these processes and frameworks will and must change over time as related technologies and their use change (M. Pollitt, 2004).

Complementing the contribution by Pollit, Ruibin et al. also provide a modified framework. Ruibin et al. include knowledge and recycling of information to the proposed framework with the intent to reduce the complexity of investigations; specifically, in terms of the relevance of the case to the processes of the investigation (Ruibin, Yun, & Gaertner, 2005). These artifacts demonstrate the natural transition of frameworks and processes from a theoretical basis to a more practitioner oriented paradigm.

Part of this transition would be the inclusion of academically based artifacts into operational standards and guidelines. Examples of these mergers can also be found in the

literature. Kent et al. integrated forensics into a NIST standard for each phase of incident response to assist in torts and prosecution (Kent, Chevalier, Grance, & Dang, 2006). In addition, Ma et al. present a model for the obtaining of evidence that centers on the chain of custody, which is typically used in criminal trials to ensure the soundness of evidence presented to a court (Ma, Wang, Zou, & Zhang, 2011).

While the inclusion of forensic processes into standards and frameworks is present in the literature, the discussion does not contain digital forensic artifacts centered on encrypted storage. This limitation includes the current best practices guides presented by various United States federal agencies. The F.B.I. Regional Computer Forensic Lab field guide for law enforcement has no inclusions or consideration into the possibility of encrypted data storage or live forensics (Federal Bureau of Investigation, 2007). The same lack of guidance on disk encryption is also seen in the United States Secret Service field guide for best practices of digital evidence (United States Secret Service, 2007). Only the NIJ guide contains some consideration to encryption, but offers no real practitioner response to the issue (National Institute of Justice, 2004, p. 8). As of this writing, these guides are the most current versions of law enforcement best practices. Figure 1 is a comparison matrix of these best practice guides.

	FBI Field Guide	US Secret Service Guide	NIJ OJP Guide
Identify participants that may have access to keys		●	●
Identify participants that may have forensic experience	●		●
Whole Disk Encryption part of Standard Proceedures			
Legal Advice on Privacy Expectations	●	●	●
Legal Advice on Business/Personal Devices			●
Legal Advice on Third Party Technology			●
Legal Advice Warrants Involving Encryption			
Live Forensics Processes			
Encryption Determination at Seizure			
Key Detection at Seizure			
Decryption Considerations			
Prosecutoral Motions			

Figure 1. Current Law Enforcement Best Practices

These organizations are considered elite in terms of forensic capability and expertise. Yet the lack of discussion regarding encryption is representative of the void in the literature supporting practitioners in the field. The research presented in the academic literature is limited to key determination and functionality of operating system embedded encryption. An example of this is Altheide, Merloni, and Zanero. Altheide et al. present a methodology for

the capture of data in a live forensics environment. In their work, the primary issue is the retrieval of information from an encrypted storage device with the keys predetermined or known in advance (Altheide, Merloni, & Zanero, 2008). This type of research artifact stands alone in the literature yet, it is needed by many of the organizations discussed.

The scarce number of artifacts specifically focused on the acquisition of evidence from encrypted hard disk drives could be the result of several reasons. The first of these reasons could be the very recent rise in disk encryption. Given that the commonality of disk encryption has increased rapidly in the last few years, current research may not have been conducted in the attempt to assist law enforcement in this area. A second reason could be the rapid edification of privacy among consumers. After the National Security Administration leaks by Edward Snowden, attention to privacy and encryption in mass media became more common as exemplified by various news and reporting sites (Baldwin, 2013; Vance, Molins, Leppard, & Zaragoza, 2015).

Within the context of these limitations and considerations, the purpose of this research is to expand the academic literature and meet the needs of practitioners who might conduct digital investigations. The goal is to provide a framework that can be used to create policy and procedure when dealing with encrypted hard disk drives in digital investigations. This framework will be then evaluated using test case scenarios to demonstrate efficacy.

Artifact

Case Leader Role. The overall aspect of the case leader does not change. The inclusion of disk encryption will possibly affect the initial participants chosen by the case leader at the start of the investigation. Modifying the initial participants will affect the investigation timeline for the case leader layer. Investigation objectives, event nature, the request initial investigation, investigation geography do not change but initial participants and investigation timeline need to be modified.

Initial participants could include additional or optional resources familiar with WDE software and techniques. These people might include personnel with access to encryption keys in organization environments that store keys. These organizations include areas where the Family Educational Rights and Privacy Act (FERPA) or Health Insurance Portability and Accountability Act (HIPAA) regulations are mandated such as educational and health care facilities respectively. The initial participants might also include faster interaction with

forensic investigators familiar with disk encryption both internal and external to the organization depending on the level of expertise.

Anytime an organization requires additional expertise, training, or personnel, the expected investigation timeline could be altered. One method for minimizing this impact is to account for WDE as part of standard practice. In this regard, standard practice would include primary and possibly secondary personnel, contacts, or services familiar with WDE.

System owner role. This layer remains in place but from the vantage of a victim or suspect being defined as the system owner. With increasing use of encryption, the system owner would release passphrase or decline to do so due to possible legal incrimination. The outlined business objectives, business and event nature, business and system process model, business geography, organization and participant relationships, as well as business and incident timeline are not modified for the purposes of WDE.

Legal advisor role. The overall role of the legal advisor does not change. The discussion of this paper centers on criminal prosecution and as such, the role of the legal advisor is paramount to the success of the investigation overall. Legal advice should be part of a standard best practices and be grounded in current legal precedent. Issues regarding expectation of privacy, personal devices on organization networks, third party technology, and the very nature of a technologically changing landscape will arise.

Legal procedures for further investigation also need to be addressed. The process and motivations at this layer remain as stated by Ieong but the inclusion of WDE adds a complexity of iteration. As an example, a warrant may be issued to search a person and their belongings. An investigator with access to tech-savvy legal advice would also need a warrant to search an electronic device seized. That warrant may need to include multiple electronic devices such as a smart phone, tablet, and laptop. The phase dealing with procedures for further investigation becomes more complex through iteration as new legal requirements may need to be sought and approved. Legal objectives, legal background and preliminary issues, legal geography, legal entities and participant, legal timeframe do not change from the original framework.

Security/System architect role. The system architect role does not change, but the framework will be altered in terms of data and function. Motivation for the system architect role will remain the same in terms of objectives, but during an investigation, organizational

policies might be in use regarding WDE. Access to these keys will probably be restricted. Investigators will need to consider this aspect when dealing with organizations that use WDE. This aspect will be one of the considerations handled by the legal advisor actor. The security domain and network infrastructure, entity model, and timing will not change in scope or definition.

Digital forensics specialist role. The role of the digital forensic specialist and the forensic investigator are often shared roles held by the same person or people. It is important to separate these functions as a sequence. The role of the digital forensic specialist is strategic in nature. The various aspects to this role often lead to specific methods to be deployed by investigators during search and seizure.

The forensic investigation strategy objective is based on the needs of the case manager. This will include case leader and legal advisor objectives from previous layers. Encryption will need to be considered at this point in order to meet these objectives. In every digital investigation, the foundation of the investigation is the need to seize and retrieve data evidence. Without considering disk encryption, this fundamental need will not be met.

The forensics data model will need to include mitigation for disk encryption. Various specific models can be used at this point to retrieve evidence. Regardless of the model utilized at this phase, WDE should be a consideration for the specialist. The model will need to be chosen by the specialist or investigator that best meets the needs of the case manager while maintaining the parameters of the strategy chosen.

The forensics data model will have a strategy design. This selected strategy is the method by which the model achieves the desired result. There may be multiple methods in this model. As an example, a model may include a combination of live forensic tools. The model may include a live forensic tool with a key detector. The model may be a combination of collection and brute force mechanics. The data model will need to be flexible, appropriate for the specific case objectives, and include mitigation of WDE.

Although forensics data geography and the forensic entity model do not change, the hypothetical forensic event timeline needs to be altered. This timeline will be structured and will be heavily dependent on the timelines of the investigator, analyst, and case manager. As these timelines are modified due to the use of disk encryption, so too will be the forensic event timeline, especially due to encryption key retrieval. This is partly due to the planning

and selecting of the appropriate model to be used during seizure. Additionally, there may be delay in obtaining or breaking the encryption key.

Forensic investigators/system administrator/operator role. The objectives of the investigator are directly driven by the case leader, legal input, organization policy, and system owner. The objectives guiding the investigator in criminal cases will vary depending on the type of offense or criminal activity being investigated. The on-site forensics data observation layer should be based on best practices in terms of methodology. For practitioners, this will follow the Department of Justice and Department of Defense guidelines. For academics, this will follow seminal and prominent literature. An example of this would be the process set forth by Department of Justice in the FBI guidelines with sequential instructions. WDE will have been considered prior to the enactment of the model method. This aspect of the artifact's design will overflow into forensic acquisition and seizure procedures as the two are closely tied and related.

Seizure procedures will need to incorporate fundamental changes to the methodology. As stated in the forensic model design, depending on the device and various circumstances, the methods used for search and seizure will vary. Method modification should include encryption detection, key detection, and be done in a forensically sound extraction. The tools and process for these goals will change over time. If the investigator has a flexible model, it allows for variances in the seizure environment. The remaining aspects of site network forensics data acquisition, participants interviewing and hearing, and forensics acquisition timeline do not change unless directly altered by the nature of the case or from one of the higher roles in the framework.

Forensic investigator/analyst role. The role of the digital forensic analyst is to provide criminal investigators or prosecutors digital evidence for the case. Forensic examination objectives are directly related to the case manager objectives. As stated earlier, in criminal cases this depends heavily on the nature of the crime being investigated or prosecuted. Once the process of decryption takes place, the major aspects to this role remain unchanged. Often the forensic investigator or analyst has the same function as the forensic investigator on site for search and seizure. Only in large law enforcement agencies are the analyst roles and the crime scene investigators typically split. As an example, the United States FBI relies on Evidence Response Teams (ERT) to secure evidence, including digital

devices that may contain evidence. The ERT does not analyze that evidence rather, it is delivered to the Regional Computer Forensics Laboratory for analysis. Often times the process of decryption comes at this stage. Decryption would be the only addition to this role. Additionally, decryption may involve an iterative sub-process with prosecution.

Prosecutor role. The prosecutor role and functions are largely unchanged. One addition to the framework for prosecutors is the possibility that decryption may not be readily available. During the course of an investigation in the United States, defendants have protection against self-incrimination as given by the Fifth Amendment to the constitution. Releasing a pass-phrase or encryption key can be self-incriminating. One legal way to challenge this is for investigators or prosecutor to seek a compel order from the court to release the passphrase. Failure to comply with the compel order places the defendant in contempt of court at which point they can be incarcerated until compliance is met. Compelled decryption is currently debated between lower courts and the Federal District Courts of Appeal. As it stands at the time of this writing, if law enforcement and prosecutors can show the court certain circumstances exist, the decryption keys can be compelled. Once the key has been discovered, the process returns to the analyst layer for additional analysis. The remaining legal presentation objectives, attributes, procedures, jurisdiction, entities, and timeline remain unchanged, as prosecution will not take place until all evidence is available and an indictment has been returned.

The nature of design science research is the production of a contributory artifact to the body of knowledge. One key element to this is the evaluation of the artifact through demonstration. Evaluation of the proposed artifact will take place using a criminal investigation in which the primary evidence source has been encrypted with WDE and the encryption key is unknown. The remaining narrative will discuss the outcome and conclusions of the artifact evaluation. This will be followed by suggestions and possible future research.

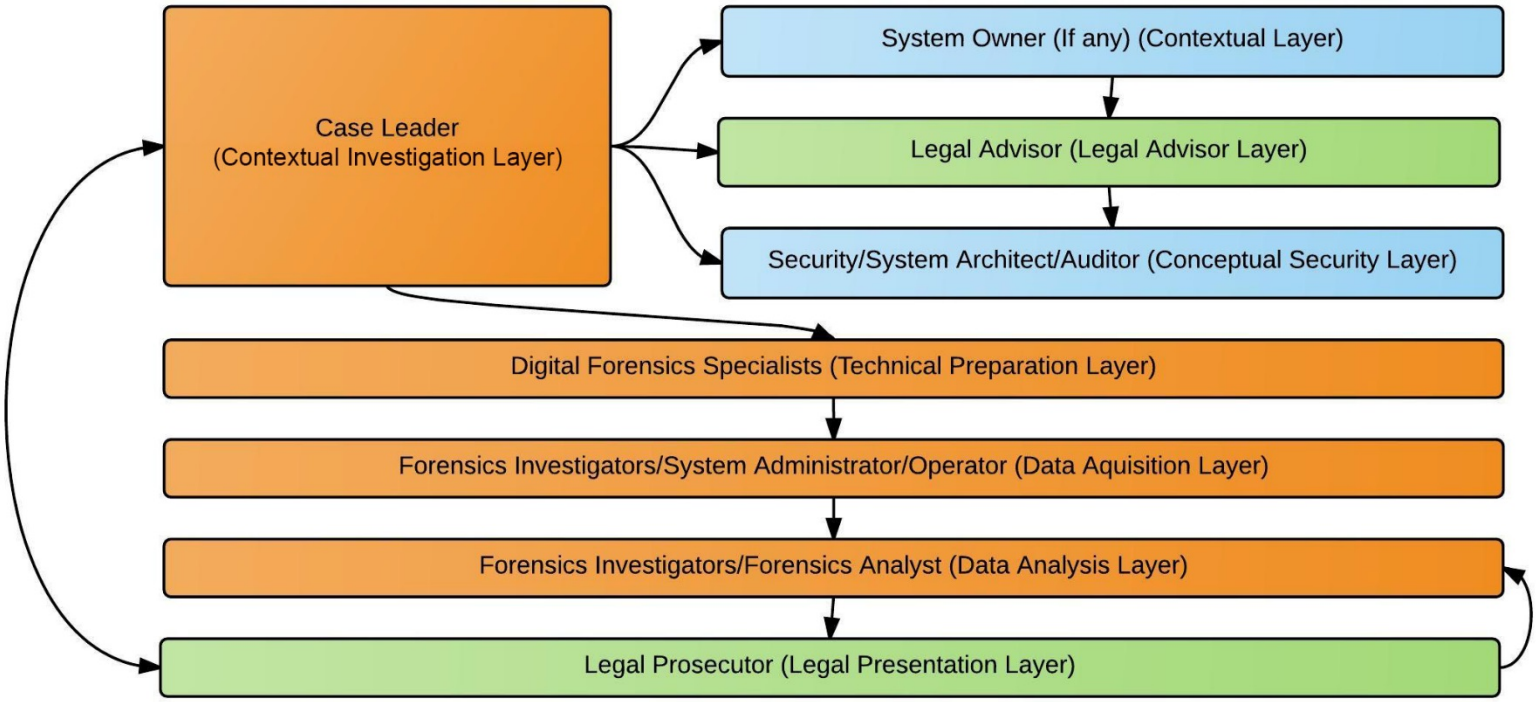

Figure 2. FORZA Process Overview by Ieong (2006)

	Why (motivation)	What (data)	How (function)	Where (network)	Who (people)	When (time)
Case leader (contextual investigation layer)	Investigation objectives	Event nature	Requested initial investigation	Investigation geography	Initial participants	Investigation timeline
System owner (if any) (contextual layer)	Business objectives	Business and event nature	Business and system process model	Business geography	Organization and participants relationship	Business and incident timeline
Legal advisor (legal advisory layer)	Legal objectives	Legal background and preliminary issues	Legal procedures for further investigation	Legal geography	Legal entities and participants	Legal timeframe
Security/system architect/ auditor (conceptual security layer)	System/Security control objectives	System information and security control model	Security mechanisms	Security domain and network infrastructure	Users and security entity model	Security timing and sequencing
Digital forensics specialists (technical preparation layer)	Forensics investigation strategy objectives	Forensics data model	Forensics strategy design	Forensics data geography	Forensics entity model	Hypothetical forensics event timeline
Forensics investigators/system administrator/operator (data acquisition layer)	Forensics acquisition objectives	On-site forensics data observation	Forensics acquisition/ seizure procedures	Site network forensics data acquisition	Participants interviewing and hearing	Forensics acquisition timeline
Forensics investigators/ forensics analysts (data analysis layer)	Forensics examination objectives	Event data reconstruction	Forensics analysis procedures	Network address extraction and analysis	Entity and evidence relationship analysis	Event timeline reconstruction
Legal prosecutor (legal presentation layer)	Legal presentation objectives	Legal presentation attributes	Legal presentation procedures	Legal jurisdiction location	Entities in litigation procedures	Timeline of the entire event for presentation

Figure 3. FORZA High Level Overview by Ieong (2006)

	FBI Field Guide	US Secret Service Guide	NIJ OJP Guide	EnFORZA
Identify participants that may have access to keys		●	●	●
Identify participants that may have forensic experience	●		●	●
Whole Disk Encryption part of Standard Proceedures				●
Legal Advice on Privacy Expectations	●	●	●	●
Legal Advice on Business/Personal Devices			●	●
Legal Advice on Third Party Technology			●	●
Legal Advice Warrants Involving Encryption				●
Live Forensics Processes				●
Encryption Determination at Seizure				●
Key Detection at Seizure				●
Decryption Considerations				●
Prosecutoral Motions				●

Figure 4. Comparison of Best Practices and Proposed EnFORZA Framework

CHAPTER 3

RESEARCH METHODOLOGY

The methodology for this research study will adhere to a foundation in the academic literature. The seminal literature of design science research is the work of Hevner et al. and Peffers et al. (Hevner, March, Park, & Ram, 2004; Peffers et al., 2007). The basis of this is to systematically approach design science research with artifact creation and evaluation being a critical step to produce contributions to the body of knowledge. Utilizing the seven guidelines put forth by Hevner et al., and the Design Science Research Method (DSRM) process model put forth by Peffers et al., this framework will mitigate the threats to validity and rigor common to design science research methodology.

The artifact creation for this research will focus on the original work setup by Ieong and the FORZA framework. The purpose for building on the FORZA framework is twofold. The first purpose is that the FROZA framework already accounts for legal issues as a primary contribution. This fits well given the legal nature of criminal cases in digital forensic investigations. Secondly, the artifact presented by Ieong is well established in the literature making modifications to the artifact more attractive to both academics and practitioners alike. The FORZA framework process flow is illustrated below. Each of the various layers will be expanded on as they related to the use of WDE.

Limitations

One of the limitations of the proposed framework is the nature of changing technology. Eventually, encryption algorithms and tools will evolve. Additionally, privacy and criminal laws may change which could render aspects of the proposed framework inadequate for the current function. The proposed framework will also assume only criminal cases in the United States where national security is not at risk. Different laws and exceptions are made in cases involving national security that may not apply to standard criminal cases. These include FISA courts and exceptions that law enforcement can make under the PATRIOT Act. The final limitation to this framework is the restriction of investigations to

traditional hard disk drives which do not include solid state drives (SSD) or NAND flash based drives. These are more common than other forms of storage and present more availability for testing.

Demonstration

Demonstration and evaluation of the proposed artifact will come from the use of a previously adjudicated criminal case. The artifact will then be executed based on the specifics of that criminal case. A previously adjudicated case was selected for multiple reasons. The first reason is that because the case has been adjudicated, or cleared from the court system, it is no longer a privacy concern and is an open public record. The second reason is that feedback from the original prosecutor and investigators regarding the framework outcome can be used to further refine the artifact. This accomplishes the iterative requirements set forth by Hevner et al. and Peffers et al. in their respective guidelines for design science research. Additionally, this process removes possible bias of the artifact author through the use of external validation by practitioners.

Demonstration of the artifact will be laid out with a review of the rubric used. An example case from the literature will then be discussed through each layer of the EnFORZA framework to show how the framework works in an investigation. Finally, the case used for demonstration will be explained per each layer and encryption consideration component. This example and demonstration of the artifact and the use of the rubric discussed below will meet the needs design science methodology as set forth by Peffers et al. (Peffers et al., 2007, p.55).

Rubric

The rubric used for validation of the framework will be based on the primary categories as outlined in figures 1 and 4. These components are the enhancements proposed by the EnFORZA framework. Each component is the adaptation of the original FORZA framework to include encryption considerations. The rubric has three levels of classification for the twelve components of the proposed framework. The highest level is the classification of exceptional, which is a best practices approach. At the exceptional level, components regarding encryption have been given consideration and includes some action or effort taken by the case manager and identified participants of the case.

The second level of classification is the acceptable level. At the acceptable level, encryption concerns and practices are being considered, but may not be acted upon by the

case manager or identified participants. This lack of action may be for a number of reasons. In some cases there may be a lack of personnel or human talent and resources. There may be a lack of financial resources or a lack of basic technology and infrastructure. Additionally, the encryption component may be considered, but not acted upon due to appropriateness of the case.

The third level is the unacceptable level. This level shows the need for reflection on the practices used by the case manager and controlling agency. If the encryption component is graded at this level, little to no consideration to the complications that encryption can add to the investigation and case have been made. This can increase the time it takes to adjudicate the case successfully. Each level and corresponding component can be viewed in table 1.

The first component is the identification of participants that may have access to encryption keys. At the exceptional level, the case manager has identified participants that may have access to encryption keys. With the identification of participants with this access, the case can proceed much more quickly should encryption be found to be in use. This will typically be the system owner in terms of the proposed framework. In larger environments, this could be an information technology manager or chief technology officer. At the acceptable level, consideration to encryption is given but no participants available with access to encryption keys or passphrases. The reason for lack of participants could be for several reasons including no identified system owner, no available system owner, or a lack of cooperation with the system owner. For criminal cases the last two can be common as discussed in the literature where cases have a deceased system owner or one that is going through the process of investigation and enacting legal rights. At the unacceptable level, there has been no consideration or identification of participants that may have access to encryption keys or passphrases. This is different from the previous levels in that consideration of encryption keys was part of the procedure for progressing with the investigation. At this level though, encryption is not a consideration at all. This can slow the investigation, prosecution, and adjudication significantly at later stages.

The second component is the identification of participants that may have forensic experience. At the exceptional level, there will be direct interaction with participants that have previous forensic experience. This may be a forensic expert on staff or through a vendor. There will be some amount of resource given to this component at this level in order to ensure

that an investigation can continue successfully. At the acceptable level, consideration is given but there are no participants available with previous forensic experience. This is a resource issue for the case manager and organization. While the desire to have access to someone with previous experience may be present, the lack of personnel, lack of training, or simply location all may play a part in keeping this from realization. At the unacceptable level, there has been no consideration given to previous forensic experience. This is a concern due to the issue that evidence may be obtained and not done so in a sound manner. Having no ability to rely on the experience of forensic personnel may compromise the case as a whole. It may jeopardize the ability to obtain information and evidence later in a worse case or prolong the case unnecessarily.

The next component to the rubric scores if encryption is part of the agency standard operating procedures. At the exceptional level, WDE is considered and expanded as part of the standard operating procedures for the department or agency in question. The consideration aspect of this would be that the case manager will consider that encryption could be in use, while at the same time preparing the evidence acquisition and forensic personnel that encryption may be in use, expanding by the preparation of other participants. At the acceptable level, encryption is considered, but there is no action or preparation by the case manager as part of standard procedures. At the unacceptable level, there is no consideration of encryption as part of standard procedures. This is an issue due to the possibility of prolonging the seizure, analysis, and investigation. By not considering encryption as part of standard procedures, the process of the investigation would need to be stopped or paused while some aspect dealing with encryption is handled. While this is not avoidable at all times due to varying circumstances, the risk of time, resources, and evidence being lost are reduced or mitigated.

Obtaining legal advice from the legal participant is paramount to a successful investigation. The legal layer of the proposed framework handles one of the most critical aspects of any investigation. The legal advice can be worked into standard procedures, but there should still be some aspect of legal counsel, be it internal to the organization or a partnership with another group such as a prosecutor in terms of a criminal investigation. In dealing with legal advice and technology, and as the case discussed earlier with Apple Inc. and the US FBI, there are many facets that a case manager will have to handle. These include

privacy expectations, business and personal devices, third party technology, and warrants specific to encryption.

The first legal component is advice regarding privacy expectations. Often times there is an expectation of privacy afforded to people in the United States. This expectation is not always absolute. There are many circumstances in which the expectation of privacy is suspended. This can occur on organization or work related computers and devices. The expectation of privacy can also be suspended once the information in question transverses a network out of the control of the system owner. Seeking advice on the scope of privacy expectations can lead to faster evidence recovery, alternate evidence gathering vectors, and proper probable cause in situations which may be more complicated such as work related machines or servers. At the exceptional level, the legal advice regarding expectation of privacy is not only sought, but utilized in the best manner possible given the nature and specifics of the investigation and case manager needs. At the acceptable level, the legal advice is considered, but either no action was taken or no action was needed. This lack of action should not be taken to mean anything other than a lack of resources or a lack of need. At the unacceptable level, there has been no consideration to the expectation of privacy. This will probably lead to additional subpoenas for information, additional motions proving to a court and a judge that privacy is not infringed, among possible others. This prolongs the investigation and continues to spend human and financial resources which could be mitigated or reduced through initial preparation.

Legal advice should also be sought regarding the issues involved with personal and business devices. This consideration is necessary in two primary ways. The first is linked to privacy issues. If a device is owned by an organization, then the organization may have suspended the right or expectation of privacy. Many organizations will cooperate fully with law enforcement upon the production of proper legal documents. If the device is a personal device, such as a laptop, operating in an organizational environment, then the issue becomes more difficult. The organization has no obligation to produce the device, and may have no legal ability to cooperate. This is only a small example of how things can become complicated as the division of organizational and private devices have merged over the last twenty years.

Other issues related to private and business devices are often overlooked. Some systems and devices are considered critical to business operations. Business that need to

maintain operational status can still be served with a warrant to search and seize. Consider servers with traditional hard disks running patient information at a hospital. In this scenario, the ability to see patients and care for them may over-rule an asset seizure. In cases like this, knowing and preparing ahead of time will limit the impact to the organization or system owner. The exceptional grade for this component would consider the paradigm of personal and business devices and utilize that information in the best manner possible. At the exceptional level, this legal advice is considered, but there is no action taken. Again, this may be to the lack of need by the case manager. While the unacceptable level denotes that no consideration is given to the private or business nature of the device. This complicates the investigation by prolonging the time it takes to move forward and any associated human or financial costs.

In dealing with third party technology, legal advice is paramount to not only the case manager's needs, but the way that an investigation can move forward. As the FBI v. Apple Inc. case has noted, the understanding of third party technology can become complicated and time consuming. Unless the case manager or forensic expert is fluent in all technology, which is unlikely, considerations for newer technology or custom devices becomes paramount. If the forensic expert has no previous knowledge about the computer then getting legal advice may prove valuable, but this complicates the investigation from a legal standpoint. Any outside expert would need to be contracted or granted some type of authority to act on behalf of the investigative organization, or at least acting under the supervision of an agent of that organization.

As an example, consider an organization running traditional servers with traditional hard disks. Servers may run custom operating systems, or at least less common one that the forensic expert may be more accustomed. Sometimes it is necessary to get the assistance of an outside expert in various operating systems and file systems to ensure no loss of data or evidence. This becomes even more complicated with the inclusion of blade devices that have dedicated hard drives but operate as a combined unit or storage. Some of these devices are simply too large to seize or may be business critical.

Given these issues, the exceptional grade for this component shows consideration of the issues possible by the case manager. Additionally, the case manager may pull or request various resources or expertise to accomplish the goal needed for the investigation to continue.

At the acceptable level, the legal advice is sought but there may not be any additional expertise needed, requiring no additional legal considerations. At the unacceptable level, there has been no consideration to third party technology. This complicates the investigation, as well illustrated by the dispute between Apple and the FBI, by prolonging the length of time it takes to retrieve evidence and continue the investigation process.

The last consideration from a legal advice perspective is the issue of warrants. Due to the way the justice system works in the United States, police cannot search the content computer without consent or without a warrant. Knowing ahead of search and seizure will assist the case manager in terms of putting the best warrant to a judge. Because encryption complicates the issue of seizure, assuming that the device is encrypted may allow for warrants to be prepared ahead of time for compelling encryption key or passphrase release. If there is enough probable cause for a search warrant, and given the state of encryption use today, there is likely enough probable cause to request passphrases and encryption keys. The exceptional level of this component is best illustrated in the same such manner. At this level, the legal advice regarding encryption for seizure in the warrant writing process is used to prepare or include encryption keys or passphrases.

At the acceptable level, the consideration for encryption keys and passphrases is given, but no action is taken at the time the warrant is prepared. One thing to consider at this point in the process is the judge. Law enforcement often, over time develop a working relationship with magistrates that sign off on warrants. If the investigator feels that the warrant may or may not be rejected, this aspect may not be included. There may also be a lack of probable cause for the warrant to include encryption as a consideration. At the unacceptable level, no consideration to encryption, either keys or passphrases, was given during the warrant writing process. This level prolongs the investigation through the need to obtain additional warrants or compel motions to access computing devices. Additionally, if the secondary or follow-up warrants have little that meets the standard for a judge, then the warrant can be rejected as a 5th Amendment protection as seen in the Boucher case (*United States v. Boucher*, 2009). If the warrant for encryption keys or passphrases is not obtained, there is not another option, the criminal case may be dropped. Fortunately, there are alternatives to the reliance of warrants alone. Forensic expertise and tools play a large role in accessing data that can be encrypted.

One of these tools available to the forensic expert participant is live forensics. Live forensics are typically software and hardware tools that allow an investigator to access evidence on a machine, in a forensically sound manner, while the machine is in operation or "live". These types of tools have become useful in that the data or evidence in question can be obtained before the system is powered off, resulting in the possibility of an encrypted state hard disk. There is a large availability of commercial and open-source live forensics suites on the Internet. The training to use such tools is still an issue for many law enforcement agencies, but availability itself does not present a challenge to investigators. For the component of facilitating live forensic processes, the exceptional level includes the use of live forensics at all possible levels of seizure. This does not include instances where the machine is already powered off. The acceptable level of live forensics is instanced where live forensics are considered, but not used. This could be due to the machine already being in the powered off state. Also, the forensic expert utilized may have limited experience in using live forensics, as training for that organization may be an issue. At the unacceptable level, live forensics is not a consideration at all. If the machine is currently powered on, there may be crucial evidence in the system memory or in part of the hard disk used for memory swap. Without live forensics, investigators may lose data that could be used in an investigation, either prolonging the investigation or ending it.

Another issue for investigators during the process of evidence seizure is key detection. While software for detecting encryption keys is still in the beginning stages of large scale use, in the future this will be a necessary tool for forensic investigators. The premise of key detection is the location of encryption keys in system memory. If the key or passphrase is found in system memory, the device can be decrypted at a later stage once powered off. This type of option could in many ways save large amounts of legal hurdles if utilized through the live forensics process. At the acceptable level, the detection of encryption keys or passphrases is used in all qualifying or appropriate seizures. Adding this to a standard operating procedure could save future investigations large amounts of time, especially if the same passphrase has been used in multiple locations or devices. At the acceptable level, the case manager or forensic expert takes into consideration key detection but takes no action. In these instances, the forensic expert may not have the required software, the machine may be powered off, or the investigation may call for something more appropriate. At the unacceptable level, there is

no consideration given to key detection. As stated prior, this makes off scene decryption more difficult for the investigation, prolonging the time to reach a case outcome.

Decryption is the next critical component. Decryption is the process by which encrypted data, or cipher-text, is translated into unencrypted data or plain text. Decryption is the stage at which the data seized can be used in the prosecution of a criminal case. Although it may seem normal to conclude that decryption would be part of the logical process of an investigation, decryption is sometimes overlooked as an integral part of evidence collection and analysis. Everything thus far in the proposed framework up to this component has revolved around retrieving decrypted or unencrypted information from a hard disk through obtaining encryption keys, passphrases, or capturing data before it leaves the decrypted state. Without the process of decryption, there may be evidence that cannot be accessed and utilized in the investigation. At the exceptional level, decryption has been considered either directly or through one of the many options in previous components and is a viable option, meaning that evidence could be retrieved. At the acceptable level, decryption is considered but not necessarily viable. A good example of these instances would be the system owner is unable to provide a passphrase or encryption key due to death or some other incapacitation. Another issue may be that although possible, the length of time it would take to brute force the decryption, typically the process of trying all possible passphrase permutations, would take too long for the investigation timeline. In these instances, which can be common, consideration is given to decryption, but it may not be viable. At the unacceptable level, there has been no consideration given to decryption. This can cause delays in the process as investigators would have to return to a previous stage to determine or obtain decryption information such as encryption keys or pass phrases in order to continue the investigation. These delays can be costly in terms of human and financial resources.

The last component is the use of motions by the prosecution. The use of additional motions are necessary as obstacles in the case may hinder the progress of the prosecution. These obstacles may include privacy issues, self-incrimination protections, or simple lack of cooperation. These obstacles may be overcome legally through the use of additional motions. By considering encryption and the associated complications that are associated with its use, motions can be preliminarily prepared and ready for filing with the court. At the exceptional level, the case manager has requested the appropriate participant to preliminary prepare

motions overcoming traditional obstacles when dealing with encryption. At the acceptable level, these motions are not preliminarily prepared but are considered when needed. While this is acceptable, it is not ideal as the motions may take additional time and efforts. At the unacceptable level, there has been consideration to prosecutorial motions related to encryption or associated complications. This can be detrimental to the case as a whole. If the obstacle cannot be overcome through a legal means, then the case charges can be dropped or withdrawn. Preliminary preparation, at some level, can assist and bring the case to an adjudication with reduced risk.

The rubric discussed previously is represented at each component and each grade level by Table 1. This rubric, along with the proposed framework will be used to discuss a case as a demonstration of the framework per the requirement made by Hevner et al.

Table 1: EnFORZA Rubric

Components	Exceptional	Acceptable	Unacceptable
Identify participants that may have access to encryption keys	Participants with possible access to encryption keys or passphrases identified.	Consideration given but no participants available with access to encryption keys or passphrases.	No consideration or identification of participants that may have access to encryption keys or passphrases.
Identify participants that may have forensic experience	Participants with previous forensic experience sought and consulted.	Consideration given but no participants available with previous forensic experience.	No consideration to forensic experience given.
Whole Disk Encryption part of Standard Procedures	WDE is considered and expanded as part of standard procedures	WDE is considered part of standard procedures	No Consideration given to encryption
Legal advice on privacy expectations	Legal advice is sought and examined as part of privacy expectations. Advice is utilized in best manner possible.	Legal advice considered for privacy expectations	No consideration given to legal advice on privacy expectations
Legal advice on business /personal devices	Legal advice is sought and examined as part of business and personal devices. Utilizing any information in best manner possible.	Legal advice considered for business / personal devices during the seizure process	No consideration given to legal advice on business/personal devices
Legal advice on third party technology	Legal advice considered for third party technology. Additional resources or expertise sought.	Legal advice is considered for third party technology	No consideration given to legal advice on third party technology
Legal advice on warrants involving encryption	Encryption considered in use during warrant writing process.	Encryption considered during the warrant writing process.	No consideration given to legal advice on warrants involving encryption
Live forensics processes	Live forensics used in all possible instances of seizure.	Live forensics considered, but not used.	No consideration given to live forensics processes
Encryption determination at seizure	Encryption determination acted upon in all qualifying seizures	Encryption determination is considered at seizure but not acted upon	No consideration given to encryption determination at seizure
Key detection at seizure	Key detection acted upon in all qualifying seizures	Key detection considered but not acted upon	No consideration given to key detection at seizure
Decryption considerations	Decryption is considered and viable	Decryption is considered but not viable	No consideration given to decryption considerations
Prosecutorial Motions	Additional prosecutorial motions are considered and preliminary prepared for possible filing with the court.	Additional prosecutorial motions are considered.	No consideration given to prosecutorial motions related to encryption

CHAPTER 4

RESULTS AND DISCUSSION

To demonstrate the proposed framework in a manner that meets the criteria set forth by Hevner et al., the case *United States v. Fricosu* (2011) will be used from the literature review. Each layer of the proposed framework will be demonstrated through the use of this case proof in three manners. The first manner will describe the original case as it is available from the documentation. This will be followed by the use of the proposed framework to obtain a more favorable or more efficient outcome. Finally, the rubric discussed in chapter 3 will be used to evaluate the use of the proposed framework. The demonstration and evaluation of the proposed framework with the Fricosu case meets the design science requirements set forth by Peffers et al in their methodology. Peffers et al. state that the demonstration will fall under Activity 4 which includes the use of simulation or case proof to solve at least one instance of the problem identified (Peffers et al., 2007, p.55). Additionally, the authors list Activity 5, the evaluation, which should measure how well the artifact assists the problem solution. These are represented by the application of the framework in narrative and the use of the rubric respectively.

Case Background

The FBI searched the home of Ramona Fricosu after a Federal Grand Jury indicted her on charges of real estate fraud in May 2010. During the execution of the warrant, Federal agents on the FBI Evidence Retrieval Team seized several computers, storage devices, and most importantly a Toshiba M305 Laptop. During evidence analysis, the FBI attained an additional search warrant to search the laptop contents. When the laptop was searched specifically pursuant to the second warrant, the government agent discovered the laptop was encrypted with PGP full disk encryption.

The United States Government then filed a motion using the All Writs Act of 1789 to compel Fricosu to aid the investigation by making the unencrypted contents available through any means that the defendant and her counsel decided. After several counter motions and an additional amicus brief was filed on behalf of the court, a list of previous passwords was

delivered to law enforcement by Fricosu's ex-husband. In July 2013, almost two years after the motion to compel, Fricosu entered a plea arrangement with United States Prosecution in which she was forfeit a vehicle, $10,233 cash seized during the initial warrant, and $912,038 in summary judgement.

Applied Framework

Applying the proposed EnFORZA framework to the example case of *United States v. Fricosu* begins with the case leader. The primary encryption consideration of the Fricosu case is that encryption was not a concern until after the laptop was seized and analysis had begun. The Case Leader in this case did not give encryption a consideration during the planning and seizure phases of the investigation. As the case leader gave no consideration to encryption, the process was stalled later while investigators relied on legal means to, unsuccessfully obtain the encryption key or passphrase.

Based on this description, the component of identifying participants would be rated as unacceptable on the validation rubric. If the case leader had considered encryption from the start of the investigation as a possibility, the scoring of the identification component could be improved. By considering encryption at the onset, the participants with access to the encryption keys or passphrases would have identified Fricosu and her ex-husband. This identification would have moved the component rubric from unacceptable to exceptional. If the case leader had given consideration to encryption, yet not identified possible participants with access to encryption keys or passphrases, the case outcome would not have changed at this stage in the investigation, but the grade on the rubric would have changed to the acceptable level.

The second component, identify participants that may have previous forensic experience, remains unchanged for this example case. The investigation was handled by FBI agents during seizure. The FBI Evidence Recovery Teams are some of the foremost experts in forensic techniques and experience. Given the nature of the investigation and the level of expertise involved, the rubric would be at the exceptional level for this component.

The next component, whole disk encryption is part of standard operating procedures, would be graded at the unacceptable level. The reasoning for this is found by the reaction of the investigators. The use of whole disk encryption was not discovered until the forensic analysis phase of the investigation. Discovery of whole disk encryption, if part of a standard

operating procedure, would begin with some initial encryption detection. The Fricosu case shows that encryption was not considered at all as part of any standard procedure through the simple failure of early detection. This process will vary by case and environment, but the decision to use some form of encryption detection, if appropriate for that specific case, would show that encryption had been considered as part of standard operating procedures.

The fourth component, legal advice regarding privacy expectations, would be graded at the acceptable level for the Fricosu case. In this instance, privacy was considered through the normal legal process of obtaining a warrant. Warrants in the United States must be worded specifically when presented to a magistrate or judge for signing. When presented for approval, a warrant must outline specifically when the warrant will be served, where the warrant will be served, what will be searched, and what is to be seized as evidence. There are methods that law enforcement can use to allow flexibility. As an example, a warrant might suggest any electronic computing devices. This level of vagueness allows law enforcement flexibility to seize various devices such as computers, laptops, console gaming systems, and smart phones. Privacy concerns are protected by the warrant writing and approval process. Because the actual warrant was unavailable for open records, the rubric level must stay at the acceptable level with the basic privacy expectations considered under the warrant review process.

The need for legal advice regarding business and personal devices was also given consideration during the warrant writing and approval process. For the Fricosu case, the warrant was served to search the Fricosu personal home. Although this may have been a home office of the defendant, it was not a third party office where Fricosu worked as an employee. Given this environment, the consideration was given to the nature of personal devices in the home. This would put the grade of acceptable for this component. If there had been a need to search a business or third party component, then additional search warrants would have been sought for locations other than the home of Fricosu.

In searching a business or organization, there is also a need to consider third party technology. Although the Fricosu case did not contain third party technology, the need is dependent on the environment and situation. If investigators are serving a warrant to a business and are unfamiliar with the environment, technology, or operations, severe damage can be done to both the evidence desired and the organization’s ability to operate. Third party technology may be as simple as bladed servers, virtual machines like Amazon’s Elastic

Compute, or cluster computing. These are not standard technologies and require specialized skills and knowledge. The case manager must decide if and how to bring those resources to the investigation. In the Fricosu case, there was no direct need for third party considerations warranting the rubric grade at the acceptable level as there was no documentation to support an unacceptable score.

The next component is the need for legal advice involving encryption. The grade for this component is unacceptable. The reasoning for this grade is the nature of the analysis. The warrant, if written with consideration to encryption, would have allowed law enforcement to search the residence for indications of passphrases. Passphrases are sometimes written on pieces of paper or stored in notebooks. A warrant with this consideration would allow the agents during the seizure to search for these documents. If the agents had been allowed to do this directly, the grading rubric would move from unacceptable, to the acceptable level. If encryption had been assumed to be in use, then not only would the warrant have consideration for encryption keys and passphrases, but there could be some action taken during seizure, possibly shortening the outcome of the investigation and moving the rubric to exceptional.

Following the legal considerations is the use of live forensics during seizure. Live forensics is not appropriate in all circumstances or environments. If the target device is already powered off, then typically law enforcement simply seizes the device as evidence. Live forensics requires the machine to be in a powered on state so that the software being run can determine processes that are running, files that are open, and the contents of memory. One key aspect to live forensics is the observation of the contents of the random access memory (RAM). The use of live forensics is an important aspect to the considerations of encryption during an investigation. Live forensics can assist with encryption determination and key detection. For the Fricosu case, live forensics was not used as is determined by the forensic analysis report. If live forensics had been used, or in this particular case, had been appropriate to use, encryption might have been detected before the end of the seizure process. It in unknown if the computer seized in the Fricosu case was powered on or off at the time of seizure, but encryption may or may not have been considered. The grade of acceptable would be given to this consideration on the rubric due to the unknown power state of the laptop as live forensics may have been an option, but inappropriate at the time.

A second aspect in which live forensics can be used is the determination of encryption use. Live forensics can determine the processes running in memory. This includes applications and processes related to whole disk encryption software. If the processes related to whole disk encryption can be detected early, then investigators can save time and effort in the case during analysis by obtaining as much data as possible prior to the device being powered down and reverting to the encrypted state. In the Fricosu case, it is unclear if live forensics was available to the agents during search and seizure, given that the machine may have already been powered down. In this particular instance, the best grade to give would be acceptable, as consideration to encryption may have been given. However, if the machine was in a powered down and encrypted state, live forensics, and therefore encryption determination would be inappropriate.

Key detection is also dependent on the use of live forensics during search and seizure. Key detection software can be part of a live forensics package and is used to obtain encryption keys or passphrases in system memory. If key detection can be used as part of the investigation process, obtaining additional warrants and compel orders may not be necessary as the investigators and prosecution may have everything needed to view evidence. This can reduce the time needed for the investigation and prosecution of any possible criminal charges. Due to the uncertain nature of the investigation in the Fricosu case regarding the use of live forensics, it remains unclear if key detection was considered. Given this circumstance, the rubric grade should be marked as acceptable based on the situational nature in the use of live forensics.

The determination of the use of encryption as well as passphrase and key detection are useful in the goal of decrypting the evidence, sometimes without the passphrase or key. This process can be achieved through various techniques. One such technique is a “brute force” attack. This type of attack, also known as an exhaustive key search, attempts every possible key permutation and can be commonly successful against weaker encryption algorithms. Some commercial forensics packages offer a decryption attack based variations of the brute force method. This can be through common or pre-generated lists of passphrases that are available on the Internet for download. If decryption has not been considered prior to seizure or during the analysis, there remains the possibility of a longer investigation process. In the Fricosu case, the decryption considerations remain unclear. The documents provided to the

court only show that during the forensic analysis, whole disk encryption was determined by the loading screen. There is no direct mention of decryption steps taken in the notes and the process may have been considered but deemed non-viable. Although the rubric grade here would be acceptable, the lack of notation regarding decryption may cause difficulties. If asking later to compel a defendant or third party, the prosecution may have to show that all viable and available options have been exhausted to a court.

Compel orders are motions before a court of law in the United States. They are one of many types of motions and are used to ask a judge or magistrate to force a person to comply with a request of the court made on behalf of the prosecution or defense in a criminal case. In the Fricosu case, additional prosecutorial motions were used to compel compliance with the search of the laptop with whole disk encryption. The rubric grade for the Fricosu case would be acceptable as there was an additional search warrant for the laptop contents and a compel motion to assist investigators under the All Writs Act of 1789. This will vary between the United States Government and the Individual States as to the nature of additional motions. The states do not have access to the same laws that the Federal Government can utilize in an investigation. As an example, the states cannot use the All Writs Act in order to compel assistance. Prosecution can accelerate the process by giving consideration to these motions prior to their absolute need. Preliminarily preparing motions for filing with the court can reduce the time needed for the prosecution to move forward, and reduce the time needed to adjudicate the case.

Findings

In discussing the example case of *United States v. Fricosu*, there is room for improvement regarding the process of a forensic investigation with consideration to whole disk encryption. In the example case, the tally was 1 exceptional, 6 acceptable, and 3 unacceptable scores on the rubric. When discussing the challenges at each level, significant improvements can be made regarding the use of whole disk encryption. The improvements can be noted with the comparison of Table 2, where the original case does not use the proposed framework, and Table 3, where the case has the framework applied as discussed prior. The improvements most significant were; the identification of participants that may have access to encryption keys, whole disk encryption part of standard procedures, and seeking legal advice on warrants involving encryption. Each of these, when addressed based

on the court records would move from the unacceptable level to the exceptional level. Excluding the component of identifying participants that may have previous forensic experience, the remaining eight components would move from the acceptable to exceptionable based on the court records obtained and the discussion prior. These remaining eight components show a moderate improvement in the processes used.

It can be demonstrated from the case discussion that without any considerations, adjudication of the criminal case will take longer. By giving consideration to each of the components in the proposed framework, the adjudication process can be demonstratively reduced through prior planning and methodical execution of the proposed framework. These improvements can show reduced time in evidence seizure, forensic data recovery, and adjudication of the criminal case through plea arrangements and trial preparation.

Table 2: Fricosu without EnFORZA

Components	Exceptional	Acceptable	Unacceptable
Identify participants that may have access to encryption keys			x
Identify participants that may have forensic experience	x		
Whole Disk Encryption part of Standard Procedures			x
Legal advice on privacy expectations		x	
Legal advice on business /personal devices		x	
Legal advice on third party technology		x	
Legal advice on warrants involving encryption			x
Live forensics processes		x	
Encryption determination at seizure		x	
Key detection at seizure		x	
Decryption considerations		x	
Prosecutorial Motions		x	

Table 3: Fricosu with EnFORZA

Components	Exceptional	Acceptable	Unacceptable
Identify participants that may have access to encryption keys	x		
Identify participants that may have forensic experience	x		
Whole Disk Encryption part of Standard Procedures	x		
Legal advice on privacy expectations	x		
Legal advice on business /personal devices	x		
Legal advice on third party technology	x		
Legal advice on warrants involving encryption	x		
Live forensics processes	x		
Encryption determination at seizure	x		
Key detection at seizure	x		
Decryption considerations	x		
Prosecutorial Motions	x		

CHAPTER 5

CONCLUSIONS

Problem Summary

There is an increase in the use and availability of encryption in today's consumer and commercial technology through both the integration with modern operating systems as well as an increase in overall awareness of encryption. There have also been changes to both legal and law enforcement practices involving the search and seizure of evidence which may include data that is encrypted. There are also increased privacy concerns given the level of integration and connectivity to the Internet today. While a useful tool to protect against common crimes like identity theft and identity fraud, the whole disk encryption of traditional hard disk drives remains a hindrance for law enforcement agencies investigating criminal cases in the United States.

This issue has been discussed in the academic literature and demonstrated in relevant criminal cases. The academic literature includes specific calls for research on this topic and the legal cases presented in the literature review show that the use of whole disk encryption is still a relevant research topic. The literature also shows that current law enforcement best practices are behind in the considerations for the use of whole disk encryption. Additionally, there is some evidence in the literature and legal cases that whole disk encryption is being used beyond the scope of privacy protection as an anti-forensic tool.

The purpose of this research is three-fold. The first is to directly answer the calls for research discussed in the literature review. These calls are academic in foundation and discuss the direct impact to practitioners and law enforcement. The second purpose is to expand the body of Information System (I.S.) knowledge through an applicable methodology. The third purpose of this research is to provide an artifact that can assist law enforcement in the United States in the investigation and prosecution of criminal acts in which whole disk encryption has been used. In the proposed research, all three of these components are met.

This research directly answers the calls set forth by Garfinkel as well as Casey et al. discussed in the extant scholarly I.S. literature. The expansion of the I.S. knowledge base is

accomplished through a completed design science artifact following the requirements set forth by Hevner et al. and Peffers et al. in their respective guides and methodologies regarding design science. Lastly, the proposed research artifact demonstrates a systematic manner in which practitioners can improve process time to a desired outcome. This proposed artifact is the focus of the discussion and findings, as well as, implications for practitioners and future research on the subject of whole disk encryption.

Discussion of Findings

The goal of any Information Systems based research is to contribute to the I.S. body of knowledge. The main contribution to the body of I.S. knowledge is the proposed EnFORZA artifact. EnFORZA provides a much needed update to the knowledge, practices, and considerations needed by practitioners in the use and mitigation of risk dealing with whole disk encryption in criminal cases. The artifact proposed also has research and scholarly based application as it can be further refined through the design science methodology for improvement over time as technology and laws change in the United States.

The artifact has a practitioner focus in that law enforcement and prosecutors can apply the considerations given in the artifact to internal processes and procedures. If the artifact is applied at the agency or organization level, improved operating procedures can be implemented to reduce the time needed to indict, prosecute, and adjudicate a criminal case. If the artifact is applied at the case level, it can be used to meet the needs of an agency or investigator on micro-level tailoring the considerations on a per-legal case basis as demonstrated in the Fricosu case. This shows that the framework is flexible and allows for application across a broad spectrum of practitioners in the United States.

Limitations

With any scholarly research, there will be limitations to the study. The proposed EnFORZA framework has some limitations discovered in the process of refinement and evaluation. The first limitation is that the demonstration case was representative only to the Federal level, which has different actions of recourse than those available to the States. The United States government has legal and investigative resources that are not shared by the states. As such, this is a limitation of the study in that no demonstration of the proposed framework was done at the state level. Demonstration of the artifact at the State level should be done as part of additional iteration and refinement of the artifact.

As a result, not all case documentation was available. The search warrant was not made available to the court in the Fricosu case. Although the examiners' forensic notes are available, the seizing of evidence plays a critical role in encryption cases. At the state level, two cases were identified that met the requirements of the proposed research in Texas and Arizona. In the Texas case, a request for assistance and open records was attempted multiple times, but agreements with local agencies were not available in regards to this publication. The second criminal case with the necessary requirements was identified in the state of Arizona, but the court documentation was not complete at the time of the evaluation activity. In order to proceed with more clarity, these documents would need to be available. Having all documentation available from the court and the investigators, which act as separate entities and agencies, will be useful and more informative in further refining of the research artifact. With more complete documentation, a demonstration at the state level can be made.

Implications for Practice

As discussed earlier, there are many implications for practitioners in using this framework for law enforcement, investigations, and prosecution. The primary contribution of the framework is to improve processes and procedures related to search and seizure, investigation, and analysis of encrypted evidence. The artifact can be used to streamline processes involved with the planning of evidence seizure where encryption could be in use. Agencies and organizations that can streamline the process of investigating a case can more easily determine the primary considerations needed for obtaining a successful adjudication. Evidence that may be encrypted in a case like Fricosu will have increased time and resources in reaching a successful prosecution or case adjudication. A reduction in resources could mean a reduction in the number of cases that go to trial, which is a costly option to the state and federal governments. Reducing the resources needed will also allow for higher conviction rates through the use of plea arrangements and possibly higher adjudication rates in cases where there is no guilt. The case will not be extended as long in either guilty or not-guilty verdicts. The artifact can also be used to assist law enforcement agencies develop a standard operating procedure for criminal cases involving traditional hard disk drives and the use of encryption technologies.

Encryption cases can also be tailored with the use of the EnFORZA framework. Should some new specific technology or new law arise, the agency can simply go back and

iterate through the framework for special needs or an adaptation. This is certainly true with changing laws. As more cases like Fricosu and the San Bernardino case illustrates, as technology changes so will the crimes in which it is used. The laws associated with those crimes, as well as, domestic intelligence will also adapt to a changing technological environment. The proposed framework provides a level of flexibility to the agencies and organizations that can utilize it.

Another implication for the use of this framework are agency interoperations and aid agreements. In many instances, agencies do not have the necessary means to investigate a computer seized, let alone one that is encrypted. In using this framework, an agency will be able to identify various weaknesses in the technical or legal capabilities of the organization. This can spawn partnerships with other agencies or entities with these capabilities or lead to mutual training opportunities. The primary notion will be the identification of these weaknesses then turn to other agencies for assistance. This is already an accepted practice on any number of law enforcement practices in the United States and is the common supporting theme in task forces. Without understanding the inherent agency weakness though, assistance will be difficult to obtain or even misapplied.

The identification of weaknesses will also lead to training opportunities. Once a weakness in capability is identified, seeking training and funding for training should be an outcome. As an example, if an agency has identified a weakness in the live forensics processes considerations, then seminar or continuing education should become a priority for officers or agents. If the organization has a weakness in identifying business or third party considerations, the same would apply, but perhaps the business or vendor can offer insight for law enforcement.

Additionally, the artifact can be used to assist prosecution in the preparing of legal motions. As an example, if the prosecution has motions partially prepared ahead of the most common encryption defenses, then time and resources can be saved in the process. This also helps defense counsel or public defenders in the plea arrangements that are commonly made. By having a standard and being prepped with legal assistance, law enforcement can expedite the time needed to file charges and bring the case to adjudication.

Lastly, the artifact can assist law enforcement and prosecution in the mitigation of risk related to the admissibility of evidence. The United States legal system has very strict rules on

what constitutes evidence and how it can be used in a legal proceeding. Those rules are beyond the scope of this discussion, but having the legal assistance as part of the framework is crucial. Evidence that is not handled properly, or that maintains its legal soundness, can be dismissed. Adding to this a layer of complexity of encryption, a technology specifically designed to obfuscate information, and the pitfalls of sound evidence become greater. Adding legal assistance, best practices, and planning can avoid this issue altogether when dealing with whole disk encryption.

Future Research

The future of this research will continue the design science iterative process. The further refinement and testing of this framework will need to be addressed. The first refinement will be the demonstration of the framework with a criminal case at the state level. This was hampered by the limitations discussed prior, but if those limitations can be overcome, this is the next logical step. If this can be done, it will add to the flexibility already demonstrated by expanding the number and nature of criminal cases in the United States.

Another possible option for further research is the inclusion of media or storage beyond traditional hard disk drives. The option of other types of storage including optical media, tape media, NAND or flash based storage, are all currently used in devices today. Additionally, there should be the expansion of this research to non-traditional computing devices, specifically mobile devices. These types of devices are well illustrated by the San Bernardino shooting case with Apple and the FBI. Given the wide spread use of mobile as a platform for digital communication, there will be more technology and legal challenges coming in the future. Being able to apply this framework to those types of storage media and mobile devices will also increase the usefulness of the artifact as well as contribute to the body of I.S. knowledge.

In addition to more types of storage and various types of devices, having a research partnership with practitioners might improve the validity of the artifact. If a research can partner with a digital forensics practitioner on criminal cases, or gleam some type of feedback through the iterative process used in design science research, there will be an improvement both in the usefulness of the artifact as well as a reduction in researcher bias. This type of feedback or evaluation could be an improved rubric or even experimental in nature.

Conclusions

What is certain about the nature of this research is that the calls for furthering it were founded and substantiated. The use of encryption is both a necessity for data protection and a hindering technology to law enforcement. Technology will change and encryption will continue to improve for consumer use. As such, law enforcement must be able to adapt to uphold law and investigate criminal activity while at the same time supporting personal privacy. Further research needs to be done on behalf of practitioners, specifically law enforcement that strengthening investigations and privacy. Frameworks, methods, and models can assist by providing practitioners the much needed tools for adapting to changing technology and laws in the United States.

REFERENCES

All Writs Act., Pub. L. No. 28 U.S.C. 1651 (1789). United States.

Altheide, C., Merloni, C., & Zanero, S. (2008). A methodology for the repeatable forensic analysis of encrypted drives. *Proceedings of the 1st European Workshop on System Security*. Glasgow, Scotland: ACM.

Apple Inc. (2012). *Best Practices for Deploying FileVault 2*. Retrieved from http://training.apple.com/pdf/WP_FileVault2.pdf

Apple Inc's Motion To Vacate Order Compelling Apple Inc. To Assist Agents In Search, And Opposition To Government's Motion To Compel Assistance (2016).

Baldwin, R. (2013). Don't Be Silly. Lock Down and Encrypt Your Smartphone. *Wired*. Retrieved October 25, 2015, from http://www.wired.com/2013/10/keep-your-smartphone-locked/

Baryamureeba, V., & Tushabe, F. (2004). The Enhanced Digital Investigation Process. *Digital Forensic Research Workshop*. Baltimore, MD.

Beebe, N. L., & Clark, J. G. (2005). A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation, 2*(2), 147–167.

BitLocker Drive Encryption in Windows 7: Frequently Asked Questions. (2012). Retrieved June 19, 2016, from https://technet.microsoft.com/en-us/library/ee449438(v=ws.10).aspx

Canetti, R., Dwork, C., Naor, M., & Ostrovsky, R. (1997). Deniable Encryption. In B. Kaliski Jr. (Ed.), *Advances in Cryptology — CRYPTO '97 SE - 6* (Vol. 1294, pp. 90–104). Springer Berlin Heidelberg.

Carrier, B. (2003). Defining digital forensic examination and analysis tools using abstraction layers. *International Journal of Digital Evidence, 1*(4), 1–12.

Carrier, B., & Spafford, E. (2004). An Event-Based Digital Forensic Investigation Framework. *DFRWS*. Baltimore, MD.

Carrier, B., & Spafford, E. H. (2003). Getting physical with the digital investigation process. *International Journal of Digital Evidence*, *2*(2), 1–20.

Casey, E., Fellows, G., Geiger, M., & Stellatos, G. (2011). The growing impact of WDE on digital forensics. *Digital Investigation*, *8*(2), 129–134.

Casey, E., & Stellatos, G. J. (2008). The impact of WDE on digital forensics. *SIGOPS Oper. Syst. Rev.*, *42*(3), 93–98.

Chan, E. M. (2011). *A framework for live forensics*. *ProQuest Dissertations and Theses*. University of Illinois at Urbana-Champaign, Ann Arbor.

Commonwealth v. Gelfgatt (2014).

Drive Crypt Plus. (n.d.). SecurStar. Retrieved from http://www.securstar.com/products_drivecryptpp.php

FIPS-197. (2001). Retrieved from http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

Fruhwirth, C. (2016). *LUKS On-Disk Format Specification Version 1.2.2*. Retrieved from https://gitlab.com/cryptsetup/cryptsetup/wikis/LUKS-standard/on-disk-format.pdf

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. *Digital Investigation*, *7*, *Supplem*(0), S64–S73.

Gasti, P., Ateniese, G., & Blanton, M. (2010). Deniable cloud storage: sharing files via public-key deniability. In *Proceedings of the 9th annual ACM workshop on Privacy in the electronic society* (pp. 31–42). New York, NY, USA: ACM.

Government's Ex Parte Application for the Order Compelling Apple Inc. to Assist Agents in Search; Memorandum of Points and Authorities (2016).

Government's Reply In Support Of Motion To Compel And Opposition To Apple Inc.'S Motion To Vacate Order (2016).

Grover, D. (2004). Dual encryption and plausible deniability. *Computer Law & Security Review*, *20*(1), 37–40.

Grover, D. (2005). Data - plausible deniability. *Computer Law & Security Review*, *21*(5), 405–407.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Q.*, *28*(1), 75–105.

Ieong, R. S. C. (2006). FORZA – Digital forensics investigation framework that incorporate legal issues. *Digital Investigation*, *3*, 29–36.

In re Grand Jury Subpoena Sebastien Boucher (2007).

Jones, T. (2015). Pregnant Mother Shot, Killed at Baton Rouge Apartment. *The Advocate*. Retrieved March 3, 2016, from http://theadvocate.com/news/12202975-123/pregnant-woman-shot-killed-overnight

Joshi, A., & Bhilare, D. S. (2014). Computer forensics and electronic evidence - Failure of competent computer forensic analysis and other computer-related acts as ineffective assistance of counsel. *Online International Interdisciplinary Research Journal*, *4*(1).

Krátký, R., Prpič, M., Čapek, T., Wadeley, S., Ruseva, Y., & Svoboda, M. (2016). *Red Hat Enterprise Linux 6.8 Security Guide*. Retrieved from https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/pdf/Security_Guide/Red_Hat_Enterprise_Linux-6-Security_Guide-en-US.pdf

Lich, B. (2016). What's New in Bitlocker? Retrieved June 19, 2016, from https://technet.microsoft.com/itpro/windows/whats-new/bitlocker

Losavio, M. M., & Keeling, D. W. (2011). Computer forensics and electronic evidence - Failure of competent computer forensic analysis and other computer-related acts as ineffective assistance of counsel. In *2011 6th IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, SADFE 2011, May 26, 2011 - May 26, 2011*. Berkeley/Oakland, CA, United states: IEEE Computer Society.

Maddox, D. (2015). In Brittney Mills murder case, encryption practices keep frustrated investigators from getting crucial cellphone data. *The Advocate*. Retrieved March 3, 2016, from http://theadvocate.com/news/acadiana/13069594-123/moore-cell-phone-encryption-is

Mocas, S. (2004). Building theoretical underpinnings for digital forensics research. *Digital Investigation*, *1*(1), 61–68.

Palmer, G. (2001). A Road Map for Digital Forensic Research. *First Digital Forensic Research Workshop (DFRWS)*. Utica, New York: AFRL/IFGB.

Peffers, K., Tuunanen, T., Rothenberger, M., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *J. Manage. Inf. Syst.*, *24*(3), 45–77.

Petroni Jr., N. L., Walters, Aa., Fraser, T., & Arbaugh, W. A. (2006). FATKit: A framework for the extraction and analysis of digital forensic data from volatile system memory. *Digital Investigation*, *3*(4), 197–210.

Pollitt, M. (2004). Six blind men from Indostan. In *First Digital Forensic Research Workshop (DFRWS)* (pp. 7–8).

Pollitt, M. M. (2007). An Ad-Hoc Review of Digital Forensic Models. In *Second International Workshop on Systematic Approaches to Digital Forensic Engineering*. Seattle, WA: IEEE.

Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. *International Journal of Digital Evidence*, *1*(3).

Ruibin, G., Yun, T., & Gaertner, M. (2005). Case-relevance information investigation: binding computer intelligence to the current computer forensic framework. *International Journal of Digital Evidence*, *4*(1), 147–167.

Schneier, B. (2007). *Applied cryptography: protocols, algorithms, and source code in C*. John Wiley & Sons, Inc.

Seidenberg, B. (2015). Family, Friends Mourn Evanston's First Murder Victim of 2015. *Chicago Tribune*. Retrieved February 12, 2016, from http://www.chicagotribune.com/suburbs/evanston/crime/ct-evr-evanston-murder-vigil-tl-0618-20150615-story.html

Trček, D., Abie, H., Skomedal, Å., & Starc, I. (2010). Advanced Framework for Digital Forensic Technologies and Procedures. *Journal of Forensic Sciences*, *55*(6), 1471–1480.

United States v. Boucher (2009).

United States v. Fricosu (2013).

United States v. Kirschner (2010).

Vance, C., Molins, F., Leppard, A., & Zaragoza, J. (2015). When Phone Encryption Blocks Justice. *New York Times*. Retrieved October 25, 2015, from http://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html

What's New in BitLocker. (2014). Retrieved June 19, 2016, from https://technet.microsoft.com/en-us/library/dn306081(v=ws.11).aspx

APPENDICES

APPENDIX A: UNITED STATES V. FRICOSU DOCUMENTATION

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Criminal Case No. 10-cr-00509-01-REB

UNITED STATES OF AMERICA,

Plaintiff,

v.

2. RAMONA CAMELIA FRICOSU,
aka Ramona Smith,

Defendant.

APPLICATION UNDER THE ALL WRITS ACT REQUIRING DEFENDANT FRICOSU TO ASSIST IN THE EXECUTION OF PREVIOUSLY ISSUED SEARCH WARRANTS

I. INTRODUCTION

The United States of America, by and through John F. Walsh, United States Attorney, and Patricia Davies, Assistant United States Attorney, hereby moves this Court under the All Writs Act, 28 U.S.C. § 1651, for an order requiring the defendant Ramona Friscosu, to assist in the execution of federal search warrants by making available the unencrypted contents of a Toshiba Laptop – Satellite M305 ("Subject Computer"), previously seized and authorized for search under warrants in 10-sw-5230-MJW and 10-sw-05377-MJW.

II. BACKGROUND

The Federal Bureau of Investigation ("FBI") currently has in its possession the Subject Computer, which was seized pursuant to a search warrant issued by this Court, in 10-sw-5230-MJW. Investigative agents also sought and obtained a further warrant to search the Subject Computer for additional items in 10-sw-05377-MJW. Initial inspection of the Subject Computer revealed that it is encrypted. Because it is encrypted, law enforcement agents are not able to examine the Subject Computer as commanded by the search warrants in 10-sw-5230-MJW and 10-sw-05377-MJW.

The Subject Computer is a Toshiba Laptop – Satellite M305, Serial # 98158161W. The Subject Computer was seized from the residence inhabited by Ms. Fricosu, her two minor children, and Ms. Fricosu's mother. At the time of seizure, the Subject Computer was resting on top of its laptop case in Ms. Fricosu's bedroom. To resolve a discovery dispute, the government's counsel previously requested of Ms. Fricosu's counsel that she provide the password to the Subject Computer. Ms. Fricosu's counsel responded, in substance, that Ms. Fricosu has no obligation to assist law enforcement, and thereafter, filed a motion seeking a copy of the encrypted drive. (Document # 101).

This Application seeks an order requiring Ms. Fricosu to make available the unencrypted contents of the Subject Computer. This could be accomplished by having the encrypted Subject Computer available in the courtroom. Upon order of the court, Ms. Fricosu could enter the password without being observed by the government, or

otherwise provide the unencrypted contents of the Subject Computer by means she chose.[1] The requested order would thus allow the agents to comply with the two prior search warrants issued by this Court.

III. DISCUSSION

A. This Court May Properly Order The Requested Relief Pursuant to the All Writs Act

The All Writs Act provides that "[t]he Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C. § 1651(a). As the Supreme Court explained, "[t]he All Writs Act is a residual source of authority to issue writs that are not otherwise covered by statute." *Pennsylvania Bureau of Correction v. United States Marshals Service,* 474 U.S. 34, 43 (1985). "The power conferred by the Act extends, under appropriate circumstances, to persons who, though not parties to the original action or engaged in wrongdoing, are in a position to frustrate the implementation of a court order or the proper administration of justice... and encompasses even those who have not taken any affirmative action to hinder justice." *United States v. New York Tel. Co.*, 434 U.S. 159, 174 (1977). Specifically, in *United States v. New York Tel. Co.*, the Supreme Court held that the All Writs Act permitted district courts to order a telephone company to effectuate a search warrant by installing

---

[1]. If the requested relief is granted, the government would arrange to have computer forensic personnel standing by to prepare a forensic image of the unencrypted version immediately. The unencrypted version could be further copied for each of the defendants.

a pen register. Consequently, this Court has the authority to order Ms. Fricosu to make available an unencrypted version of the Subject Computer to effectuate the previously issued search warrants in 10-sw-5230-MJW and 10-sw-05377-MJW.

The government obtained the Subject Computer in conformity with the Fourth Amendment; that is, by application to this court for search warrants based upon a probable cause showing. This court issued two search warrants, referenced above, for the Subject Computer. This court should now issue the order requested because doing so would enable agents to comply with this court's warrants commanding that the Subject Computer be examined for evidence identified by the warrants. Examining the Subject Computer further in its current state to attempt access to its unencrypted contents, if it is possible at all, would require significant resources and may harm the Subject Computer.

B. Any Fifth Amendment Right of Defendant Is Properly Addressed by "Act of Production Immunity"

1. Facts Relevant to Fifth Amendment Analysis

As an initial matter, the following facts are worth noting:

First, the government knows that the encrypted drive exists on Ms. Fricosu's laptop computer because it was validly obtained by search warrant and is in the government's possession. The government also has sound bases to believe that the Subject Computer contains evidence relevant to the charged offenses. The charged offenses were facilitated substantially by computers. Moreover, "back up" electronic

storage devices also obtained during the search contain documents relating to the charged wire fraud, bank fraud and false statement offenses.

Second, Ms. Fricosu's voluntary conduct has linked her to the contents of the encrypted drive. It was found on the floor of her bedroom sitting on top of its laptop case. And, as set forth in the application and affidavit in 10-sw-05377-MJW, Ms. Fricosu discussed the Subject Computer with co-defendant and ex-spouse Scott Whatcott while he was incarcerated (and the telephone call was being recorded) and referenced specific information relevant to the case that the Subject Computer contains.

Third, the government already possesses, in an encrypted format, Ms. Fricosu's drive. This is not a situation where the government seeks to compel a defendant to produce items that may potentially be incriminatory and her act of producing them arguably has evidentiary value to authenticate the items.

Fourth, the government only requires that Ms. Fricosu's produce the contents of the drive in an unencrypted format. The government does not request that Ms. Fricosu give the government access to the password to the drive, either orally or in written form.

Fifth, as discussed further below, it is undisputed that the contents of Ms. Fricosu's encrypted drive are not protected under the Fifth Amendment because the files were created voluntarily and prior to the execution of the search warrants in 10-sw-05230-MJW and 10-sw-05377-MJW.

2. Defendant's Fifth Amendment Right Vis-a-vis Producing The Unencrypted Contents is Limited

The Government needs access to the unencrypted contents of the digital media in order to effectuate this Court's prior search warrants. In essence, although the government has complied with the Fourth Amendment in obtaining the Subject Computer, defendant thwarts lawful investigation. It is beyond cavil that the contents of the encrypted drive were created and compiled voluntarily and therefore do not enjoy Fifth Amendment protection simply because they may prove incriminatory or may in some way add to the government's case. *See Baltimore City Dep't of Soc. Servs. v. Bouknight*, 493 U.S. 549, 555 (1990); *In re: Grand Jury Subpoena to Sebastian Boucher*, 2009 WL 424718 (D. Vt. February 19, 2009) (involving an encrypted computer), *citing Fisher v. United States*, 425 U.S. 391 (1976) and *Doe v. United States*, 487 U.S. 201 (1988). The court should ignore any suggestion that the contents of the Subject Computer are protected simply because they may be incriminatory.

In *United States v. Hubbell*, 530 U.S. 27 (2000), the Supreme Court gave guidance regarding the scope of Fifth Amendment protection. There, the government had no knowledge of the existence or whereabouts of subpoenaed documents. *Id.* at 45. In fact, when the grand jury issued the subpoena, the government was investigating a matter entirely different from the charges ultimately brought. *Id.* at 31-32. The subpoena itself required the production of 11 "broadly worded" categories of documents and the defendant ultimately produced 13,120 pages following the granting of immunity. *Id.* at 42. The government later attempted to prosecute for different crimes based in

part of evidence developed from information contained in the documents that the defendant produced. In affirming dismissal of the indictment, the Court held that the immunity granted in the prior prosecution in exchange for disclosure precluded subsequent unrelated prosecution because the testimonial aspect of defendant's act of production was a necessary first step in discovering evidence supporting the second prosecution. The Court described the broad subpoena as the equivalent of "a detailed written interrogatory or a series of oral questions at a discovery deposition." *Id.* at 41-42.

This case shares none of *Hubble*'s defining characteristics. The government knows that an unencrypted version of the drive exists on the defendant's laptop. The government knows that the Subject Computer has a very high likelihood of containing evidence pertaining to the charged crimes for the reasons noted above. The government knows that the defendant had access to, and control over, the Subject Computer immediately prior to the search warrant execution because it was found in her bedroom, on top of the laptop case.

3. The Government Requests That This Court Order Act of Production Immunity To Address Defendant's Limited Fifth Amendment Right

As the act of production might potentially entitle Ms. Fricosu to assert her right to refuse under the Fifth Amendment of the United States Constitution, the Government has sought approval to seek this court's grant of limited immunity, thus precluding the Government from using her act of producing the unencrypted contents against her in

any prosecution.[2] No other basis exists upon which Ms. Fricosu might legally assert the right to refuse to provide the unencrypted contents. (A proposed order will be submitted prior to any hearing on this Application).

Only when an "act of production" explicitly or implicitly communicates facts or information otherwise protected by the Fifth Amendment privilege against testimonial self-incrimination – for example, if the existence and location of subpoenaed records are unknown to the Government, or where the mere act of production would authenticate the records – does the act of production fall within the scope and protection of the defendant's Fifth Amendment privilege. *See Fisher*, 425 U.S. at 409-411 (holding that production of documents within possession of taxpayer's attorneys did not implicate the taxpayer's Fifth Amendment privilege; where the "existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers"); *Doe*, 487 U.S. at 210-215 (holding that the target of a fraud investigation could be compelled to sign consent to allow foreign banks to release his banking records, since signing of the consent form itself communicated no information to the Government).

---

[2]This Application is made with approval from Kenneth A. Blanco, Deputy Assistant Attorney General of the Criminal Division of the Department of Justice, pursuant to the authority vested in him by Title 18, United States Code, Section 6003(b), and Title 28, Code of Federal Regulations, Section 0.175(a). A copy of the document from the Deputy Assistant Attorney General expressing such approval is attached hereto as Exhibit A.

The only Court that has specifically considered whether a target may be compelled to provide the unencrypted contents of a computer seized pursuant to a warrant ruled the target had no act of production privilege to refuse to provide the Grand Jury with an unencrypted version of the hard drive of his computer (by entering his password information), since "providing access to the unencrypted drive 'adds little or nothing to the sum total of the Government's information' about the existence and location of files that may contain incriminating information." *Boucher*, *supra*, 2009 424718 WL at *3-4 (*quoting Fisher*, 425 U.S. at 411*). Cf. United States v. Kirschner*, 2010 WL 1257355 (E.D. Mich. March 30, 2010) (finding that a subpoena which required target to actually respond to questioning and provide verbal testimony regarding his password did implicate the target's Fifth Amendment privilege). The *Boucher* Court noted, however, that the Government could not make use of the target's act of production to authenticate the unencrypted drive or its contents; essentially holding that the subpoena implicitly conferred upon the target limited use immunity for the act of producing the unencrypted contents of the seized computer. *Boucher*, *supra,* 2009 424718 WL at *3-4 . Thus, requiring Ms. Fricosu to provide the Government with access, by entering the necessary encryption keys to the digital media that the Government already possesses pursuant to a valid search and seizure warrant, amounts to compelling Ms. Fricosu only "to surrender the key to a strongbox containing incriminating documents." *Fisher*, 425 U.S. at 408, n. 9.

Public interests will be harmed absent requiring defendants to make available unencrypted contents in circumstances like these. Failing to compel Ms. Fricosu

amounts to a concession to her and potential criminals (be it in child exploitation, national security, terrorism, financial crimes or drug trafficking cases) that encrypting all inculpatory digital evidence will serve to defeat the efforts of law enforcement officers to obtain such evidence through judicially authorized search warrants, and thus make their prosecution impossible.

WHEREFORE, the United States of America respectfully requests that the Court issue an Order granting the Application Under the All Writs Act to require Ms. Fricosu to produce the unencrypted contents of the Subject Computer, and granting her act of production immunity in connection therewith.

Dated this 6th day of May, 2011

JOHN F. WALSH
United States Attorney

By: s/Patricia Davies
PATRICIA DAVIES
Assistant United States Attorney
United States Attorney's Office
1225 17th Street, Suite 700
Denver, CO 80202
Phone: 303/454-0100
Fax: 303/454-0401
patricia.davies@usdoj.gov
Attorney for Government

CERTIFICATE OF SERVICE

I hereby certify that on this 6nd day of May, 2011, I electronically filed the foregoing **APPLICATION UNDER THE ALL WRITS ACT REQUIRING DEFENDANT FRICOSU TO ASSIST IN THE EXECUTION OF PREVIOUSLY ISSUED SEARCH WARRANTS** with the clerk of the Court using the CM/ECF system which will send notification of such filing to the following email addresses:

Mark Johnson
mark.johnson68@gmail.com

Philip L. Dubois
dubois@dubois.com

Tonya Andrews
Tonya.Andrews@usdoj.gov

Martha Paluch
Martha.Paluch@usdoj.gov

By: s/ Maureen Carle
MAUREEN CARLE
Legal Assistant
1225 Seventeenth Street, Suite 700
Denver, Colorado 80202
Telephone: (303) 454-0100
Facsimile: (303) 454-0406
E-mail: Maureen.Carle@usdoj.gov

USA v. RAMONA FRICOSU
CASE #: 1:10-CR-00509-REB-02

APPLICATION UNDER THE ALL WRITS ACT REQUIRING DEFENDANT FRICOSU TO ASSIST IN THE EXECUTION OF PREVIOUSLY ISSUED SEARCH WARRANTS

EXHIBIT 01

U.S. Department of Justice

Criminal Division

Assistant Attorney General *Washington, D.C. 20530*

MAY - 5 2011

The Honorable John F. Walsh
United States Attorney for the
District of Colorado
1225 Seventeenth Street
Suite 700
Denver, Colorado 80202

Attention: Patricia Davies
Assistant United States Attorney

Re: *United States v. Ramona Fricosu*

Dear Mr. Walsh:

Pursuant to the authority vested in me by 18 U.S.C. § 6003(b) and 28 C.F.R. § 0.175(a), I hereby approve your request for authority to apply to the United States District Court for the District of Colorado for an order, pursuant to 18 U.S.C. §§ 6002-6003, requiring Ramona Camelia Fricosu to give testimony or provide other information in the above matter and in any further proceedings resulting therefrom or ancillary thereto, provided that the testimony or other information from such individual may be necessary to the public interest, and that such individual refuses to testify or provide information on the basis of the privilege against self-incrimination.

Sincerely,

Lanny A. Breuer
Assistant Attorney General

KENNETH A. BLANCO
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

CASE NO.: 10-cr-00509-REB

CASE CAPTION: USA v. 2-Ramona Fricosu

EXHIBIT LIST OF: Plaintiff / USA

(Name and Party Designation)

EX. NO./LTR	DESCRIPTION	STIP	IN	OUT	COMMENTS
1	Evidence Inventory		✓		11/1/11, for limited purposes of this hearing
2	Room M - Search Docs (Toshiba M305)		✓		11/1/11 "
2A	Room M - Search - Fricosu items		✓*		*Pages 1-4, 11/1/11, "
2B	Toshiba M305 - PGP screens		✓		11/1/11 "
3	Search sketches		✓		11/1/11 "
4A	Room J - Search - Dell		✓		11/1/11 "
4B	Room J - Search - Toshiba L455		✓*		*Page 12, 11/1/11; Page 11, 1/3/12
5	Rooms T & U				"
6A	Room L - Search - Gateway		✓		11/1/11 "
6B	Room L - HP Pavillion desktop		✓		11/1/11 "
7	HP Pavillion laptop docs		✓*		*Pages 1, 3, 11/1/11; Page 2, 1/3/12
7A	Correspondence re HP laptop				"
8	Transcript of 5/15/10 call		✓		11/1/11 "
9	Recording of 5/15/10 call		✓		11/1/11 "
10	Summary chart		✓		11/1/11, as redacted, "

CASE NO.: 10-cr-00509-REB-2

CASE CAPTION: United States v. Ramona Fricosu

EXHIBIT LIST OF: United States - Plaintiff
(Name and Party Designation)

PAGE NUMBER: 2 of 2

EX. NO./LTR	DESCRIPTION	*STIP*	IN	OUT	COMMENTS
11	Declaration of Travis Johnson w/ Att. 1- 7 Att. 1- Curriculum vitae Att. 2- Windows XP setup screenshot Att. 3- Registry Report [Govt. Ex. 7, pg. 2] Att. 4- Registry Report [Govt. Ex. 4B, pg. 11] Att. 5- Johnson review notes Att. 6- Registry Editor screenshot - HP laptop Att. 7- Registry Editor screenshot - Toshiba Laptop		✓		1/3/12, as redacted on the record

TABLE OF CONTENTS

STATEMENT OF AMICUS CURIAE 1

INTRODUCTION 1

FACTUAL BACKGROUND 2

A. Statement of Relevant Facts 2

B. Encryption is an Important Measure to Protect Security and Privacy 2

ARGUMENT 5

A. The Act of Entering a Password or Otherwise Decrypting Data on a Computer is a Compelled Testimonial Act Protected By The Fifth Amendment. 6

B. Neither the Encryption Password Nor the Decrypted Contents of the Laptop Is a Foregone Conclusion. 8

C. Limited "Act of Production" Immunity is Not Coextensive With Fricosu's Fifth Amendment Privilege Unless It Extends to Evidence on the Laptop Derived From Disclosure of the Password. 11

CONCLUSION 13

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Judge Robert E. Blackburn

Criminal Case No. 10-cr-00509-01-REB

UNITED STATES OF AMERICA,

Plaintiff,

v.

2. RAMONA CAMELIA FRICOSU,

Defendant.

BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF DEFENDANT FRICOSU'S OPPOSITION TO GOVERNMENT'S APPLICATION UNDER THE ALL WRITS ACT REQUIRING DEFENDANT TO ASSIST IN THE EXECUTION OF PREVIOUSLY ISSUED SEARCH WARRANTS

TABLE OF AUTHORITIES

FEDERAL CASES

Doe v. United States,
487 U.S. 201 (1988) (*Doe I*) 6, 8, 11

Fisher v. United States, 425 U.S. 391 (1976) 6, 8, 9, 10, 11

Hoffman v. United States, 341 U.S. 479 (1951) 8

In re Grand Jury Subpoena to Sebastien Boucher,
2:06-mj-91, 2007 WL 4246473 (D. Vt. Nov. 29, 2007) (*Boucher I*) ..... *passim*

In re Grand Jury Subpoena to Sebastien Boucher,
2009 WL 424718 (D. Vt. Feb. 29, 2009) (*Boucher II*) ..... *passim*

In re Harris,
221 U.S. 274 (1911) 9

Kastigar v. United States,
406 U.S. 441 (1972) 12, 13

United States v. Doe,
465 U.S. 605 (1984) (*Doe II*) 7

United States v. Hubbell,
530 U.S. 27 (2000) (*Hubbell I*) ..... *passim*

United States v. Hubbell,
167 F.3d 552 (D.C. Cir. 1999) (*Hubbell II*) 9

United States v. Kirschner,
No. 09-MC-50872, 2010 WL 1257355 (E.D. Mich. March 30, 2010) 5

United States v. Rogozin,
09-CR-379, 2010 WL 4628520 (W.D.N.Y. Nov. 16, 2010) 5

FEDERAL STATUTE

28 U.S.C. § 1651 2

CONSTITUTIONAL AMENDMENT

U.S. CONST. AMEND. V ..... *passim*

she is forced to supply information that will give prosecutors access to files they speculate will be helpful to their case but cannot identify with any specificity. And while Fricosu has been offered limited immunity, it is not enough to defeat her Fifth Amendment privilege against self-incrimination.

FACTUAL BACKGROUND

A. Statement of Relevant Facts

The government has indicted defendants Ramona Fricosu and Scott Whatcott on various charges arising from allegedly fraudulent real estate transactions. (Dkt. 1.) On May 14, 2010, the government executed search warrants at the residence that Fricosu shares with her mother and two children, and formerly shared with her co-defendant Scott Whatcott. The government seized, among other items, several computers and storage devices containing digital information. One of the seized computers was a Toshiba Satellite M305 laptop. The government obtained an additional search warrant to search this laptop, but discovered that it was unable to read the encrypted contents of the computer.

On May 6, 2011, the government filed an application under the All Writs Act, 28 U.S.C. § 1651, asking the Court to compel Fricosu to type her encryption password into the laptop. (Dkt. 111.) Specifically, the government contends, "Ms. Fricosu could enter the password without being observed by the government, or otherwise provide the unencrypted contents of the [laptop] by means she chose." Gov. App. at 2-3.

B. Encryption is an Important Measure to Protect Security and Privacy

Encryption is a process by which a person can change plain, understandable information into unreadable letters and numbers using a mathematical algorithm. Only someone with a special code—an encryption key or password—is able to decipher the

STATEMENT OF INTEREST OF AMICUS CURIAE

The Electronic Frontier Foundation ("EFF") is a non-profit, member-supported digital civil liberties organization. As part of its mission, EFF has served as counsel or amicus in key cases addressing user rights to privacy, free speech, and innovation as applied to the Internet and other new technologies. With more than 14,000 dues-paying members, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age, and publishes a comprehensive archive of digital civil liberties information at one of the most linked-to web sites in the world, www.eff.org.

EFF's interest in this case is the sound and principled application of the Fifth Amendment to encryption passwords and encrypted information stored on computers. Encryption is a widely used and fundamental safeguard for businesses and individuals who store data on portable devices like laptops, which may be easily lost or stolen. EFF submits this brief to help the Court apply the Fifth Amendment privilege against self-incrimination in a manner that ensures the constitutional rights of those who use this technological measure to protect their privacy and security.

INTRODUCTION

The government seeks to force defendant Ramona Fricosu to enter a password into a laptop or otherwise provide access to encrypted data stored on that computer. The government hopes this information will include evidence of allegedly criminal activity it can use to prosecute this case.

The Court should reject the government's application because it is contrary to the Constitution, long-standing Supreme Court precedent, and sound public policy. The government makes an aggressive argument here that may have far-reaching consequences for all encryption users. Fricosu will be made a witness against herself if

information to make it readable again.[1] Computer and software manufacturers consider disk encryption a basic computer security measure and include disk encryption tools as a standard feature on most new computers.[2] Among other things, encryption is extremely useful for protecting information on small, portable devices like laptops, which can easily be stolen or lost.[3] Typically, encryption protects sensitive information on these devices from unauthorized access, even if a lost or stolen device is never recovered. Encryption helps to ensure that data is not misused if it falls into the wrong hands.

Encryption is increasingly recognized as a critical way for companies to secure

---

[1] *See generally* Encryption, https://secure.wikimedia.org/wikipedia/en/w/index.php?title=Encryption&oldid=433989373 (last visited July 8, 2011).

[2] For example, the Microsoft Windows operating system has come with the Bitlocker Drive Encryption feature since 2008. *See, e.g.*, Microsoft, Bitlocker Drive Encryption Overview, http://technet.microsoft.com/en-us/library/cc732774.aspx (last visited July 7, 2011). The four most recent versions of Apple's Mac OS X 10 operating system have included FileVault, which is a program that allows users to encrypt files in their home folder. FileVault, https://secure.wikimedia.org/wikipedia/en/w/index.php?title=FileVault&oldid=437137960 (last visited July 8, 2011). The company plans to introduce a more sophisticated full-disk encryption feature in a new OS release later this month. Apple Insider, *Inside Mac OS X 10.7 Lion: FileVault Full Disk Encryption and Cloud Key Storage* (Feb. 28, 2011), http://www.appleinsider.com/articles/11/02/28/inside_mac_os_x_10_7_lion_file_vault_full_disk_encryption_and_cloud_key_storage.html.

[3] *See, e.g.*, Rich Phillips, *BP Loses Laptop With Private Info on 13,000 People*, CNN.com (March 29, 2011), http://articles.cnn.com/2011-03-29/us/bp.lost.laptop_1_deepwater-horizon-oil-spill-laptop?_s=PM:US; Neil Versel, *VA Laptop Incidents Show Why Encryption Is So Important*, Fierce Mobile Health Care, (Sept. 21, 2010) http://www.fiercemobilehealthcare.com/story/latest-va-laptop-incidents-show-why-encryption-so-important/2010-09-21; Paul McNamera, *Latest "Lost" Laptop Holds Treasure-Trove of Unencrypted AT&T Payroll Data*, Network World (June 5, 2008), http://www.networkworld.com/community/node/28453; Bob Sullivan, *Lost IRS Laptop Stored Employee Fingerprints*, MSNBC.com (June 5, 2006), http://www.msnbc.msn.com/id/13152636/ns/technology_and_sciencesecurity/t/lost-irs-laptop-stored-employee-fingerprints/; Robert Ellis Smith, *Laptop Hall of Shame*, Forbes.com (Sept. 7, 2006), http://www.forbes.com/2006/09/06/laptops-hall-of-shame-cx_res_0907laptops.html.

data on their computers, which can range from proprietary business information like trade secrets to sensitive customer information like credit card numbers. According to a 2010 study by Intel and the Ponemon Institute, 329 public and private organizations collectively reported more than 86,000 laptops stolen or missing over a 12-month period—an average of 263 laptops per organization. *The Billion Dollar Lost Laptop Problem* at 1 (Sept. 30, 2010).[4] Forty-six percent of those organizations said that they lost laptops with sensitive or confidential information, while 30 percent of the lost laptops had full-disk encryption. *Id.* at 6. Intrusions into computers by outsiders have also put unencrypted personal information at risk.[5] It is therefore not surprising that an increasing number of businesses consider full-disk encryption a priority,[6] which means that more and more employees encrypt the contents of their work computers.[7]

Encryption also provides critical protection for data stored on individuals' personal computers. People keep vast amounts of information on their digital devices, which might include years of correspondence with friends, family members, and colleagues; personal photographs and videos; Internet browsing histories; financial

---

[4] Available at http://newsroom.intel.com/servlet/JiveServlet/download/1544-8-3132/The_Billion_Dollar_Lost_Laptop_Study.pdf.

[5] *See*, *e.g.*, Reuters, *Thousands of Citi Customers at Risk After Hacker Attack* (June 9, 2011), http://www.msnbc.msn.com/id/43335996/ns/business-personal_finance/t/thousands-citi-customers-risk-after-hacker-attack; Jason Schreier, *Sony Hacked Again; 25 Million Entertainment Users' Info at Risk*, Wired.com (May 2, 2011), http://www.wired.com/gamelife/2011/05/sony-online-entertainment-hack.

[6] *New DigitalPersona Survey Shows SMBs Consider Disk Encryption a Priority*, Small Business Trends, (June 25, 2011) http://smallbiztrends.com/2011/06/survey-smbs-disk-encryption.html.

[7] Indeed, several states now encourage or even require businesses to use encryption to safeguard information they collect. Colorado law, for example, requires companies to notify state residents when their unencrypted personal data has been compromised and possibly misused. C.R.S. 6-1-716. Massachusetts has taken an even stronger stance, requiring everyone who owns or licenses personal data about state residents to encrypt all personal data stored on laptops and portable storage devices. *See* Mass. General Law Chapter 93H and regulations promulgated by the Office of Consumer Affairs and Business Regulation at 201 CMR 17.00.

information; sensitive medical details; and confidential work-related information. People may carry this data with them every day on laptops, tablets, and phones that could be left behind in a taxi, stolen at a café, or inspected by a prying acquaintance.

As businesses and individuals alike recognize the need to protect the privacy and security of the information on their computers, more and more people will find themselves in Fricosu's situation: facing a government attempt to force them to turn over an encryption password or a decrypted version of the data stored on a computer. Very few courts have considered whether such compulsion violates the Fifth Amendment privilege against self-incrimination. The Court should address this question with deliberation and care because it involves fundamental constitutional rights.

ARGUMENT

The Fifth Amendment provides that "no person . . . shall be compelled in any criminal case to be a witness against himself[.]" U.S. CONST. AMEND. V. Not surprisingly, the few courts to consider the question have found that this right prevents the government from forcing a witness to testify to a password used to restrict access to files on a computer. *United States v. Rogozin*, 09-CR-379, 2010 WL 4628520 at **5-6 (W.D.N.Y. Nov. 16, 2010); *United States v. Kirschner*, No. 09-MC-50872, 2010 WL 1257355 at **3-4 (E.D. Mich. March 30, 2010).

This case presents a slightly different question, which is whether the government can compel a witness to type a password into a laptop or otherwise provide access to encrypted data stored on that computer. *See In re Grand Jury Subpoena to Sebastien Boucher*, 2:06-mj-91, 2007 WL 4246473 at *6 (D. Vt. Nov. 29, 2007) (*Boucher I*), *appeal sustained by* 2009 WL 424718 (D. Vt. Feb. 29, 2009) (*Boucher II*). Under the circumstances of this case, the answer is no.

Decrypting data on a computer is a testimonial act that receives the full

protection of the Fifth Amendment. This act would incriminate Fricosu because it might reveal she had control over the laptop and the data there. The government has failed to show that the existence and location of the information it seeks is a foregone conclusion. Furthermore, the limited immunity offered by the government is not coextensive with the scope of Fricosu's privilege. The Court should therefore find that the government has failed to take the steps necessary to secure Fricosu's Fifth Amendment rights and deny the application.

A. The Act of Entering a Password or Otherwise Decrypting Data on a Computer is a Compelled Testimonial Act Protected By The Fifth Amendment.

The Fifth Amendment generally protects a person from being compelled to give testimony that would incriminate her. *United States v. Hubbell*, 530 U.S. 27, 34 (2000) (*Hubbell I*); *Fisher v. United States*, 425 U.S. 391, 408 (1976). The privilege is limited to testimonial evidence, or a communication that "itself, explicitly or implicitly, relate[s] a factual assertion or disclose[s] information." *Doe v. United States*, 487 U.S. 201, 210 (1988) (*Doe I*). Put a different way, the privilege protects the "expression of the contents of an individual's mind." *Id.* at 210 n.9; *see also* 220 n.1 (Stevens, J., dissenting). To illustrate this principle, the Supreme Court has explained that a witness might be "forced to surrender a key to a strongbox containing incriminating documents," but not "compelled to reveal the combination to a wall safe." *Id.* at 210 n.9; *see also* 219 (Stevens, J., dissenting). Forcing an individual to supply a password necessary to decrypt data is more like revealing the combination to a wall safe than to surrender a key: the witness is being compelled to disclose information that exists in her mind, not to hand over a physical item. *Boucher I*, 2007 WL 4246473 at *4.[8]

[8] Despite the fact that *Boucher II* sustained the government's appeal of *Boucher I*, the earlier decision was well reasoned and is worth consideration. In that case, a grand jury issued a subpoena to compel the defendant to enter a password to allow the government access to encrypted files on a particular drive on a computer. 2007 WL

The fact that the witness might type the information into a keyboard rather than speak it out loud does not change that basic fact. The act of disclosing information may be so testimonial that the privilege applies to the production itself. *United States v. Doe*, 465 U.S. 605 (1984) (*Doe II*). An act of production has a sufficiently testimonial aspect to trigger Fifth Amendment protection when it forces a witness to admit the existence of papers, the fact that they were in her possession or control, and that they were authentic. *Hubbell I*, 530 U.S. at 36 (citing *Doe II*, 465 U.S. at 613 (internal quotation marks omitted)).

Forcing Fricosu to enter the laptop password into the computer or otherwise decrypt the data stored on the computer meets this standard because the act of doing so will imply assertions of fact. *See Hubbell I*, 530 U.S. at 37. The act would be an admission that she had control over the computer and the data stored on it before it was seized from her residence—which are critical admissions, particularly considering that she shared her residence with her co-defendant. The act would also show that she knows the encryption password and was able to access the encrypted data. If Fricosu knows the password, forcing her to perform the act of decrypting the data on the laptop will put her in the "cruel trilemma" that the privilege is designed to protect against:

4246473 at *1. A magistrate judge determined that entry of the password was a testimonial act with which the government's grant of immunity was not coextensive, and the foregone conclusion doctrine did not apply. *Id.* at **3-6. The government subsequently modified the subpoena so that it did not seek to force the defendant to turn over his password, but instead provide the grand jury a decrypted version of the contents of the drive. *Boucher II,* 2009 WL 424718 at *1. The court upheld the subpoena as modified, finding that the defendant had no privilege to refuse to turn over the decrypted data because the government already knew of the existence and location of the files at issue. *Id.* at *4. Thus, *Boucher II* analyzed a different request for information than *Boucher I*, and while the defendant's motion to quash the modified subpoena was ultimately denied and the government's appeal sustained, most of *Boucher I*'s analysis was not overruled by *Boucher II* (but see footnote 9 *infra)*.

having to choose between incriminating herself, lying under oath, or refusing to answer and risking contempt of court. *Doe I*, 487 U.S. at 212; *Boucher I*, 2007 WL 4246473 at *3.

Even if the act were not so directly incriminating, the privilege applies not only where an act of production would itself incriminate a witness, but also to an act "which would furnish a link in the chain of evidence needed to prosecute the claimant for a federal crime." *Hubbell I*, 530 U.S. at 38 (quoting *Hoffman v. United States*, 341 U.S. 479, 486 (1951) (internal quotation marks omitted)). It appears undisputed that the encrypted data the government hopes to access might incriminate Fricosu. Gov. App. at 4. This is a vital consideration where she has been indicted on more than 30 counts since the government seized the laptop, regardless of the fact that the government has agreed not to use the act of producing the decrypted data against her. As explained below, this immunity offer is inadequate under the circumstances of this case.

B. Neither the Encryption Password Nor the Decrypted Contents of the Laptop Is a Foregone Conclusion.

The government contends that the existence and location of the decrypted contents of the laptop are a forgone conclusion because incriminating evidence might be found there. Gov. App. at 7 & 9. This argument misconstrues the foregone conclusion doctrine in a dangerous way, and the Court should not accept this interpretation of the law.

When the existence and location of information are known to the government, and the witness "adds little or nothing to the sum total of the Government's information by conceding that [s]he in fact has the [information]," those matters are treated as a "foregone conclusion." *Fisher*, 425 U.S. at 411. Under those circumstances, "no constitutional rights are touched. The question is not of testimony but of surrender." *Id.* citing *In re Harris*, 221 U.S. 274, 279 (1911). In situations where the foregone

conclusion doctrine applies, the government typically already has extensive information about the material it seeks. *United States v. Hubbell*, 167 F.3d 552, 576 (D.C. Cir. 1999) (*Hubbell II*), *aff'd Hubbell I*, 530 U.S. 27. The government's knowledge of the existence, control, location and authenticity of the information must be nearly the same as the witness's for the doctrine to overcome the privilege. *Id.* at 576-78.

The government has not made that showing here. It claims that the laptop "has a very high likelihood of containing evidence pertaining to the charged crimes," Gov. App. at 7, that the "charged offenses were facilitated substantially by computers," Gov. App. at 4, and that other digital storage devices seized from the home Fricosu shared with Whatcott contained documents relating to the charged offenses, Gov. App. at 4-5. But a "very high likelihood" is nothing more than an educated guess. The government can identify neither specific evidence it expects to find on this particular laptop, nor where this supposed evidence might be found on the computer. This is not a situation in which the password will "add[] little or nothing to the sum total of the Government's information[.]" *Fisher*, 425 U.S. at 411. To the contrary, compelling Fricosu to supply the information will add a great deal to the government's knowledge that it does not already have.

Only one case has addressed a similar legal question, and the facts here are so different that they require a different result.[9] *Boucher II* considered whether the defendant could be forced to turn over a decrypted version of data stored in a particular drive on a laptop. 2009 WL 424718 at **1-2. In that case, the defendant had already acknowledged to the government that he owned the computer. *Id.* at *1. He had displayed the contents of some of the files, revealing that they likely included images or videos of child pornography. *Id.* at **1-2. The government independently searched for

[9] To the extent that *Boucher II* overrules *Boucher I*, it is likely on this question. *Boucher II*, 2009 WL 424718 at **3-4.

and located files they suspected were child pornography. *Id.* at *2. The defendant also accessed a particular drive on the computer in a government agent's presence, where the agent located and examined several files that appeared to be contraband. *Id.* Under the circumstances, the court concluded that providing the government access again to the files on the drive "add[ed] little or nothing to the sum total of the Government's information about the existence and location of files that may contain incriminating information," and was therefore a foregone conclusion. *Id.* at *3 (citing *Fisher*, 425 U.S. at 411) (internal quotation marks omitted).

Unlike the investigators in *Boucher II*, government agents here have never viewed any data on the laptop. The government contends that Fricosu discussed a laptop with Whatcott in taped conversations, Gov. App. at 5, but has not shown that the laptop seized from the residence is the same laptop mentioned in these discussions. Even assuming the government could show that it is the same laptop, it can identify neither files relevant to this investigation nor their location on the computer.[10]

The facts of this case are more like those in *Hubbell I*. In that case, the government issued a subpoena ordering the defendant to produce eleven categories of documents, which the defendant had to help produce. 530 U.S. at 41. Noting that the government could independently prove neither the existence nor the whereabouts of the documents produced in response to the subpoena, the Court rejected the argument that the papers' existence and location were a foregone conclusion. 530 U.S. at 44-45. In particular:

---

[10] To the extent the government seeks to force Fricosu to type a password into the computer, as *Boucher I* notes, the foregone conclusion doctrine likely does not apply. 2007 WL 4246473 at *6. Assuming Fricosu has no written record of the password, it exists only in her mind (if she knows it at all). Compelling her to type the information into a computer "is pure testimonial production rather than physical evidence having testimonial aspects," and the foregone conclusion document would not come into play. *Id.*

> The documents did not magically appear in the prosecutor's office like "manna from heaven." They arrived there only after [the defendant] . . . took the mental and physical steps necessary to provide the prosecutor with an accurate inventory of the . . . potentially incriminating evidence sought by the subpoena.

Id. at 42. So too is the case here. What the government might find on the laptop is not a foregone conclusion, but only will be available to the government if Fricosu can supply the information necessary to produce a decrypted version of the data.

The government suggests that this case is analogous to *Fisher* and *Doe I*. Gov. App. at 8. But those cases are easily distinguishable on the facts. In *Fisher*, the government was able to confirm the existence and authenticity of subpoenaed documents through an independent third party who also possessed copies of them. 425 U.S. at 402. As the Supreme Court explained, "[C]ompelled production of documents from an attorney does not implicate whatever Fifth Amendment privilege the taxpayer might have enjoyed from being compelled to produce them *himself*." *Id.* (emphasis added). Here, there is no indication that an independent third party can provide the information sought. And in *Doe I*, the Supreme Court found that it was constitutional to compel a witness to sign a consent directive that did not confirm the existence of a specific foreign bank account or authenticate any records that might be in the possession of a foreign bank. 487 U.S. at 215-16. In contrast, forcing Fricosu to provide the information necessary to decrypt the data on the laptop will directly link her to the computer and the data on it.

C. Limited "Act of Production" Immunity is Not Coextensive With Fricosu's Fifth Amendment Privilege Unless It Extends to Evidence on the Laptop Derived From Disclosure of the Password.

The government seeks the Court's approval to grant Fricosu "limited immunity" to prevent the government from using the act of producing the unencrypted data against her in any prosecution. Gov. App. at 7-8. Specifically, this immunity will not permit the

government to use the *act* of production against Fricosu, but apparently will allow the government to use the data actually obtained through the act of production against her, as well as any evidence the government learns as a result of accessing that information. This limited immunity does not defeat Fricosu's Fifth Amendment privilege against self-incrimination because it is not "coextensive with the scope of the privilege." *Kastigar v. United States*, 406 U.S. 441, 453 (1972); *Boucher I*, 2007 WL 4246473 at *5.

When a witness's act of production is testimonial in character, the government must grant use and derivative-use immunity to satisfy the Constitution's requirements. *Hubbell I*, 530 U.S. at 41-46. This means that the government may not use the act of production itself against Fricosu, nor any evidence on the computer derived from the act of production. *Kastigar*, 406 U.S. at 453. As the Supreme Court has explained, use and derivative-use immunity "prohibits the prosecutorial authorities from using the compelled testimony in *any* respect, and it therefore insures that the testimony cannot lead to the infliction of criminal penalties on the witness." *Id.* (emphasis original).

Should the Court decide that Fricosu must supply the data on the laptop in decrypted form, the government will face a "heavy burden of proving that all of the evidence it proposes to use [from the laptop] was derived from legitimate independent sources." *Id.* at 461-62. Placing this burden on the government ensures that the grant of immunity leaves the prosecutors and witness "in substantially the same position as if the witness had claimed [her] privilege in the absence of a grant of immunity." *Hubbell I*, 503 U.S. at 40, citing *Kastigar*, 406 U.S. at 458-59 (internal quotation marks omitted).

The government's offer of limited immunity—with no guarantee against use or derivative use of the information Fricosu would be forced to supply—is not comprehensive enough to secure Fricosu's Fifth Amendment rights. She is therefore justified in refusing to provide the password. *Kastigar*, 406 U.S. at 449.

CONCLUSION

The government is overreaching to try to compel Fricosu to supply an encryption password that they hope will give them access to the full contents of a laptop. The Court should decide this important constitutional question in a way that recognizes the substantial benefits of encryption to safeguard the security and privacy of digital information stored on computers. New technologies present new challenges for law enforcement, but this reality does not justify the abandonment of well-established constitutional protections that secure individuals' rights. Decrypting data is an act with testimonial aspects that are protected by the Fifth Amendment. The government cannot identify the evidence it hopes to find with any specificity, and it has not offered Fricosu immunity coextensive with her Fifth Amendment privilege against self-incrimination. For all the reasons discussed above, the government's application should be denied.[11]

DATED: July 8, 2011

Respectfully submitted,

/s/ Marcia Hofmann

Marcia Hofmann (California Bar No. 250087)
Hanni Fakhoury (California Bar No. 252629)
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x. 116
Facsimile: (415) 436-9993
marcia@eff.org
hanni@eff.org

Attorneys for Amicus Curiae
Electronic Frontier Foundation

[11] If the Court wishes to hear oral argument from EFF on the issues raised in this brief, undersigned counsel is happy to address any concerns or questions the Court may have. Counsel for EFF is unavailable on the July 22, 2011 hearing date currently scheduled for this motion, but would be willing to appear at a later date if convenient for the Court.

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO
Judge Robert E. Blackburn

Date: November 1, 2011

Deputy Clerk: Nel Steffens
Court Reporter: Tracy Weir

Criminal Action No. 10-cr-00509-REB

Parties:	*Counsel:*
UNITED STATES OF AMERICA, Plaintiff, v.	Patricia Davies Jeremy Sibert
2. RAMONA CAMELIA FRICOSU, a/k/a Ramona Smith, Defendant.	Philip Dubois

---

COURTROOM MINUTES

Hearing on Government's Application [#111]

1:45 p.m. Court in session.

Appearances of counsel. Also seated at government's table is FBI Special Agent, Scott Shons.

Defendant is present on bond.

Opening statements by the court.

Court's sequestration order is in effect.

Ms. Davies asks that FBI agent Shons be allowed to remain at government's table as advisory witness.

Response by Mr. Dubois.

Reply by Ms. Davies.

IT IS ORDERED as follows:

1. That the government's request that Mr. Shons be allowed to remain at government's table as advisory witness, is **GRANTED** and that the defendant's objection is **OVERRULED**.

1:50 p.m. Opening statement/argument by Ms. Davies.

Mr. Dubois declines the opportunity for opening statement/argument.

1:54 p.m. Government's witness, Scott Schons, called and sworn.

Direct examination by Ms. Davies.

***Exhibits Identified**: Government's Exhibit 10, Government's Exhibit 2, Government's Exhibit 9, Government's Exhibit 8, Government's Exhibit 1, Government's Exhibit 3, Government's Exhibit 2A, Government's Exhibit 2B, Government's Exhibit 6A, Government's Exhibit 6B, Government's Exhibit 7*

***Exhibits Admitted**: Government's Exhibit 2; Government's Exhibit 9; Government's Exhibit 8;Government's Exhibit 1; Government's Exhibit 3; Government's Exhibit 2A, Pages 2-4; Government's Exhibit 2B, Government's Exhibit 6A, Government's Exhibit 6B, Government's Exhibit 7, Page 1*

Parties stipulate that Room M on May14, 2010, was the bedroom of Ms. Fricosu.

3:10 p.m. Court in recess.

3:26 p.m. Court in session.

Government's witness Schons has resumed the witness stand.

Ms. Davies offers authority as discussed prior to the break.

Continued direct examination by Ms. Davies.

***Exhibits Identified**: Government's Exhibit 7, Page 3; Government's Exhibit 4A; Government's Exhibit 4B, Pages 11 & 12*

***Exhibit Admitted:** Government's Exhibit 7, Page 3; Government's Exhibit 4A; Government's Exhibit 4B, Page 12, Government's Exhibit 10, as redacted sua sponte by the court*

Parties stipulate that Room J was the room occupied by Elena Vasadi.

4:01 p.m. Cross examination by Mr. Dubois.

Exhibits Identified: *Fricosu Exhibit I, Fricosu Exhibit J, Fricosu Exhibit K, Fricosu Exhibit L, Fricosu Exhibit M, Fricosu Exhibit N, Fricosu Exhibit G, Fricosu Exhibit P, Fricosu Exhibit Q, Fricosu Exhibit R, Fricosu Exhibit S, Fricosu Exhibit T, Fricosu Exhibit U, Fricosu Exhibit E, Fricosu Exhibit D, Fricosu Exhibit V, Fricosu Exhibit W, Fricosu Exhibit C, Fricosu Exhibit F, Fricosu Exhibit X, Fricosu Exhibit H, Fricosu Exhibit A, Fricosu Exhibit B*

IT IS FURTHER ORDERED as follows:

2. That this hearing is **CONTINUED** to Tuesday, **January 3, 2012, at 8:30 a.m.**, the court reserving, if necessary, the balance of that morning to complete this hearing, at which the defendant, counsel, the government's witness and advisory witness, and the witnesses subpoenaed by the defense shall again appear without further notice, order, or subpoena; and

3. That the defendant's bond is continued.

5:01 p.m. Court in recess.

Total time in court: 03:00

Hearing continued.